

Hơn 77.000 máy tính tại Việt Nam bị mã hóa dữ liệu tổng tiền

19:27 29/05/2023

Một trong những biện pháp các đơn vị cần lưu ý để tránh bị tấn công mã hóa dữ liệu là cần đánh giá an ninh các dịch vụ trước khi mở ra Internet.



Ảnh minh họa

Theo thông tin từ Bkav, vào đầu tháng 5/2023, một doanh nghiệp lớn, có đội ngũ quản trị viên dày kinh nghiệm, nắm rõ hệ thống của mình bị mã độc mã hóa tổng tiền – ransomware tấn công, với toàn bộ hơn 10TB dữ liệu bị mã hóa. Hacker đã yêu cầu hơn 4 tỷ đồng đổi lấy chìa khóa giải mã. Vấn đề là, hệ thống của đơn vị này không được bảo vệ bởi một phần mềm diệt virus đủ mạnh.

Tiếp đó, vào giữa tháng 5/2023, một doanh nghiệp khác bị hacker tấn công và mã hóa dữ liệu hàng loạt máy chủ, máy cá nhân lúc nửa đêm. Hacker đòi 9 nghìn USD tiền chuộc dữ liệu cho mỗi máy bị mã hóa. Các chuyên gia của Bkav phát hiện, hệ thống đã bị tấn công bởi virus mã hóa Jianliang, chưa từng xuất hiện trước đây.

Hệ thống giám sát virus của Bkav còn phát hiện, dòng mã độc mã hóa dữ liệu “STOP/DJVU” hoặc “FARGO3” chuyên nhắm tới các doanh nghiệp, đơn vị sử dụng các phần mềm quản lý dữ liệu kế toán. Theo thống kê, có tổng cộng 261 máy chủ bị xâm nhập từ hơn 6.000 địa chỉ IP khác nhau.

Đáng chú ý, trong 6 tháng từ tháng 12/2022 đến hết tháng 5/2023, Trung tâm hỗ trợ kỹ thuật của Bkav đã tiếp nhận hàng trăm cuộc gọi, đề nghị xử lý mã độc mã hóa tổng tiền. Hệ thống giám sát virus của Bkav cũng ghi nhận hơn 77.000 máy tính tại Việt Nam bị mã hóa dữ liệu.

Tổng giám đốc Trung tâm nghiên cứu mã độc của Bkav -ông Nguyễn Tiến Đạt cho biết, trong số hàng trăm trường hợp liên hệ Bkav yêu cầu trợ giúp, có tới hơn 50% tổ chức, cá nhân không sử dụng phần mềm diệt virus hoặc cài đặt những ứng dụng bảo vệ không đủ mạnh.

Đặc biệt, có những đơn vị có rất nhiều dữ liệu quan trọng nhưng lại tiết kiệm, sử dụng những phần mềm diệt virus miễn phí. “Phần mềm diệt virus miễn phí có khả năng xử lý những loại mã độc thông thường, chỉ phù hợp bảo vệ những dữ liệu không quá quan trọng do không có khả năng tự động phát hiện và diệt triệt để các dòng virus mã hóa dữ liệu”, chuyên gia Bkav phân tích.

Các loại mã độc mã hóa dữ liệu sử dụng rất nhiều cách thức để tấn công như khai thác lỗ hổng dịch vụ web, dò quét mật khẩu (Brute force) vào các dịch vụ SQL, lỗ hổng hệ điều hành, để tấn công trực tiếp vào máy chủ. Cách khác là tấn công vào một máy cá nhân, từ đó âm thầm rà quét, thọc sâu vào các server và các máy tính khác trong mạng...

Để tránh bị tấn công mã hóa dữ liệu, các chuyên gia khuyến nghị người dùng và quản trị hệ thống cần thường xuyên backup dữ liệu quan trọng; không mở cổng dịch vụ nội bộ ra Internet khi không cần thiết. Đồng thời, cần đánh giá an ninh các dịch vụ trước khi mở ra Internet và cài đặt phần mềm diệt virus đủ mạnh để được bảo vệ thường trực.

Hà Trần (Th)