

180.000 máy tính trong các cơ quan tổ chức nhiễm mã độc APT

14:46 15/12/2022

Theo kết quả “Đánh giá an ninh mạng dành cho người sử dụng cá nhân” do Tập đoàn BKA V thực hiện tháng 12/2022, 180.000 máy tính trong các cơ quan, tổ chức Việt Nam bị nhiễm mã độc APT trong năm qua. Con đường phát tán chủ yếu vẫn là gửi email với nội dung dụ dỗ hoặc thúc giục mở file đính kèm.



Ảnh minh họa. (Ảnh: internet)

Thống kê của BKA V cho thấy, 180.000 máy tính trong các cơ quan, tổ chức Việt Nam bị nhiễm mã độc APT trong năm qua. Con đường phát tán chủ yếu vẫn là gửi email với nội dung dụ dỗ hoặc thúc giục mở file đính kèm.

Mã độc kích hoạt ngay khi người dùng mở file, từ đó âm thầm hoạt động trên máy tính nạn nhân: Cài đặt thêm các module thành phần khác để điều khiển từ xa, đánh cắp dữ liệu, leo thang đặc quyền, lợi dụng thiết bị để tiếp tục hành vi tấn công len sâu hơn vào hệ thống của cơ quan, tổ chức...

Để lẩn tránh các giải pháp bảo mật, mã độc sử dụng rất nhiều kỹ thuật tinh vi như DLLSideLoading (ẩn nấu dưới các phần mềm hệ thống, phần mềm nổi tiếng như Google, Office, Antivirus), fileless (kỹ thuật tàng hình), được lập trình bằng nhiều ngôn ngữ khác nhau, CVE, bootkit, rootkit...

PV (t/h)