

Năm 2023, người dùng Việt Nam thiệt hại gần 18.000 tỷ đồng do virus máy tính

14:22 21/01/2024

Hiện nay, tình hình an ninh mạng trong nước vẫn nổi cộm nhiều vấn đề nóng khi tấn công bằng virus mã hóa dữ liệu tiếp tục gia tăng, nhắm vào các máy chủ trọng yếu; máy tính không có kết nối internet cũng có thể bị tấn công gián điệp APT (Advanced Persistent Threats); lừa đảo tài chính trực tuyến không có dấu hiệu hạ nhiệt bởi nguồn cơn là tài khoản ngân hàng rác,...



Ảnh minh họa (Ảnh: internet)

Theo báo cáo khảo sát an ninh mạng của Bkav ghi nhận tỷ lệ người dùng nhận được tin nhắn, cuộc gọi lừa đảo tiếp tục gia tăng. Nếu năm 2022, con số này là 69,6% thì trong năm 2023 là 73%. Lừa đảo tài chính qua mạng bùng nổ trong những năm gần đây và trở thành vấn nạn khi nạn nhân thuộc mọi tầng lớp và sinh sống ở bất cứ đâu.

Điển hình, trong các vụ việc lừa đảo với mục đích tài chính, kẻ xấu yêu cầu người dùng chuyển tiền qua tài khoản ngân hàng. Nhưng khi điều tra, các tài khoản này đều không chính chủ, khiến cơ quan chức năng gặp khó khăn để tìm ra tội phạm và ngăn chặn vấn nạn lừa đảo. Các chuyên gia của Bkav phân tích,

tài khoản ngân hàng rác là nguồn cơn của vấn nạn lừa đảo tài chính qua mạng tại Việt Nam thời gian qua.

Năm 2023, hệ thống giám sát và cảnh báo virus của Bkav ghi nhận có tới 745.000 máy tính bị nhiễm virus đánh cắp tài khoản (Facebook, ngân hàng), tăng 40% so với năm 2022. Phát tán mạnh nhất phải kể đến các dòng như RedLineStealer, ArkeiStealer, Fabookie... đều nằm trong top 20 dòng virus lây nhiễm mạnh ở Việt Nam.

Theo kết quả khảo sát của Bkav, tại Việt Nam có tới 53% máy tính sử dụng phần mềm crack, dẫn tới việc, khoảng 10% người dùng tại Việt Nam bị mất tài khoản mạng xã hội, email, ngân hàng...

Các dòng virus đánh cắp tài khoản chủ yếu lây lan qua các phần mềm bị bẻ khóa (crack). Năm 2023, hệ thống giám sát và cảnh báo virus của Bkav cũng ghi nhận hơn 19.000 máy chủ bị tấn công mã hóa tổng tiền từ 130.000 địa chỉ IP độc hại trên toàn thế giới, tăng 35% so với năm 2022. Các dòng virus điển hình tham gia những đợt tấn công này phải kể đến TOP/DJVU, FARGO, LockBit...

Dự báo trong năm 2024, sự phát triển nhanh chóng của AI không chỉ mang lại những lợi ích rõ ràng mà còn tạo ra những nguy cơ đáng kể cho an ninh mạng.

Tuy nhiên, thách thức lớn nhất đối diện với công nghệ AI ngày nay là lừa đảo và tấn công có chủ đích APT, với mức độ ngày càng phức tạp của các kịch bản lừa đảo, đặc biệt khi kết hợp giữa Deepfake và GPT. Khả năng thu thập và phân tích dữ liệu người dùng thông qua AI cho phép tạo ra những chiến lược lừa đảo tinh vi, khiến việc nhận diện lừa đảo sẽ khó khăn hơn đối với người dùng.

PV(t/h)