| | |
|---|---|
| **ỦY BAN NHÂN DÂN**<br>**XÃ THẠCH LẠC** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập – Tự do – Hạnh phúc** |
| Số:533 /UBND-VP<br>V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 3/2026 | *Thạch Lạc, ngày07 tháng 4 năm 2026* |

Kính gửi:

- Các phòng, ngành chuyên môn UBND xã;
- Các đơn vị sự nghiệp trên địa bàn.

Trong tháng 3/2026, trên không gian mạng xuất hiện nhiều chiến dịch tấn công mạng tinh vi, lợi dụng các lỗ hổng bảo mật nghiêm trọng trên các phần mềm, ứng dụng phổ biến. Qua hệ thống giám sát an ninh mạng, đã ghi nhận nhiều loại mã độc nguy hiểm có khả năng xâm nhập, chiếm quyền điều khiển hệ thống, đánh cắp dữ liệu và thực hiện mã hóa dữ liệu để tống tiền với các hình thức, thủ đoạn

**I. Các nguy cơ tấn công mạng phổ biến**

1. Lừa đảo chiếm quyền tài khoản Zalo qua "bình chọn cuộc thi"

- Mức độ: Đặc biệt nghiêm trọng.

- Hình thức: Các đối tượng lừa đảo Gửi link giả mạo các cuộc thi qua tin nhắn Zalo yêu cầu đăng nhập để bình chọn. Khi nạn nhân nhấn vào link và đăng nhập để "bình chọn", kẻ tấn công sẽ chiếm được mã OTP hoặc phiên đăng nhập đề kiểm soát tài khoản. Sau đó đối tượng mạo danh chủ tài khoản để nhắn tin mượn tiền, lừa đảo người thân trong danh bạ hoặc tiếp tục phát tán link mã độc để mở rộng mạng lưới nạn nhân.

- Yêu cầu:

+ Tuyệt đối không nhấn vào các đường link lạ, đặc biệt là các yêu cầu đăng nhập lại tài khoản Zalo.

+ Kích hoạt xác thực 02 lớp.

+ Thường xuyên vào mục "Lịch sử đăng nhập" để đăng xuất khỏi các thiết bị lạ.

+ Xác thực trực tiếp: Nếu nhận được tin nhắn mượn tiến, phải gọi điện thoại video và các hình thức tương tự khác để xác nhận danh tính trước khi chuyển khoản.

2. Chiếm đoạt Facebook/Messenger bằng Deepfake

- Mức độ: Rất nghiêm trọng.

- Hình thức: Kẻ tấn công gửi các link gắn tiêu đề gây sốc (như tin buồn gia đình, lộ clip nhạy cảm …) để đánh cắp thông tin đăng nhập Facebook. Sau khi chiếm quyền điều khiển, đối tượng sử dụng công nghệ AI để giả dạng hình ảnh và giọng nói của chủ tài khoản thực hiện các cuộc gọi video ngắn với người thân nhằm mục đích vay tiền. Công nghệ AI khiến nạn nhân dễ tin tưởng hơn vì thấy đúng khuôn mặt và nghe đúng giọng nói của người thân.

- Yêu cầu:

+ Thiết lập thêm tính năng xác thực 02 yếu tố

+ Thiết lập danh sách "Liên hệ tin cậy" để lấy lại tài khoản khi bị sự cố.

+ Khi nhận cuộc gọi video hỏi mượn tiền mà hình ảnh chập chờn, giọng nói ngắt quãng hoặc yêu cầu chuyển tiền vào số tài khoản lạ (không trùng tên) cần ngắt máy và liên lạc qua kênh khác để kiểm tra.

3. Mã độc giả mạo ứng dụng Chính phủ

- Mức độ: Rất nghiêm trọng.

- Hình thức: Đối tượng dẫn dụ người dùng qua Zalo/Facebook để cài đặt các tệp tin lạ (Áp) giả mạo ứng dụng VNeID, Tổng cục Thuế hoặc Cổng dịch vụ công. Sau khi cài đặt, mã độc sẽ xin quyền "Accessibility Service" (Hỗ trợ tiếp cận). Nếu người dùng đồng ý, kẻ tấn công sẽ chiếm toàn bộ quyền điều khiển điện thoại từ xa, tự động đọc mã OTP ngân hàng, theo dõi thao tác bàn phím và âm thầm chuyển tiền khỏi tài khoản ngân hàng của nạn nhân mà không cần tương tác trực tiếp.

- Yêu cầu:

+ Tuyệt đối không cài đặt ứng dụng qua đường link gửi từ người lạ hoặc các tệp Áp rời. Chỉ cài đặt ứng dụng từ CH Play hoặc App Store.

+ Kiểm tra quyền ứng dụng: Vào Cài đặt, hỗ trợ tiếp cận, tắt tất cả các ứng dụng lạ đang sử dụng quyền này.

+ Nếu nghi ngờ đã cài nhầm mã độc: Ngay lập tức ngắt kết nối Internet (Wifi/4G), khôi phục cài đặt gốc của điện thoại và thực hiện đổi mật khẩu ngân hàng, Zalo, Facebook trên một thiết bị sạch khác.

**II. Cảnh báo từ hệ thống giám sát mã độc**

1. Bật tính năng hiển thị đuôi tệp tin, không mở file lạ từ USB/email. Hiển thị đuôi file để nhận diện các tệp có đuôi lạ. Tăng cường giám sát PowerShell/CMD. Cảnh giác với các tệp tin nhận từ nguồn lạ qua Email/USB.

2. Virus qua file Excel (Macro). Không bật "Enable Macros" với file không rõ nguồn. Cấu hình chặn macro trong hệ thống.

3. Mã độc trong file AutoCAD. Không mở file thiết kế không rõ nguồn gốc. Kiểm tra, làm sạch hệ thống định kỳ.

4. Mã độc gián điệp đánh cắp dữ liệu: Quét virus toàn bộ hệ thống; đổi mật khẩu và bật xác thực 2 lớp. Không lưu mật khẩu trên trình duyệt.

5. Nguy cơ từ file.exe không rõ nguồn gốc: Không tải, cài phần mềm lậu/crack. Không chạy file .exe không rõ nguồn. Tăng cường kiểm soát thiết bị USB.

Để chủ động phòng ngừa các hành vi lừa đảo trên không gian mạng, UBND xã đề nghị các phòng, ngành chuyên môn; các đơn vị sự nghiệp thực hiện các nội dung sau:

- Thường xuyên rà soát toàn bộ hệ thống máy tính, thiết bị công nghệ thông tin; triển khai cài đặt, cập nhật phần mềm diệt virus bản quyền.

- Tăng cường tuyên truyền trên hệ thống truyền thanh để nâng cao nhận thức cho cán bộ, đảng viên và người dân cảnh giác khi tiếp cận thông tin trên không gian mạng.

- Khi phát hiện dấu hiệu tấn công mạng, báo cáo kịp thời về Công an tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, SĐT: 099.338.6777) để được hỗ trợ.

UBND xã yêu cầu các phòng, ngành chuyên môn; các đơn vị sự nghiệp nghiêm túc thực hiện./.

***Nơi nhận:***
- Như trên;
- Chủ tịch, các PCT UBND xã;
- Thôn trưởng các Thôn trên địa bàn;
- Lưu: VT.

**TM. ỦY BAN NHÂN DÂN**
**KT CHỦ TỊCH**
**PHÓ CHỦ TỊCH**

U.B.N.D XÃ THẠCH LẠC T.HÀ TĨNH

**Nguyễn Đức Hải**