BỘ CÔNG AN
CÔNG AN TỈNH GIA LAI

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 3745 /CAT-PA05

Gia Lai, ngày 01 tháng 11 năm 2025

V/v cảnh báo mã độc nguy hiểm

Kính gửi:

- Văn phòng Tỉnh ủy tỉnh Gia Lai;
- Văn phòng UBND tỉnh Gia Lai;
- Bộ Chỉ huy quân sự tỉnh;
- Các sở, ban, ngành trên địa bàn tỉnh Gia Lai;
- UBND cấp xã.

Quá trình rà soát trên không gian mạng, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an phát hiện tập tin độc hại mang tên "DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.rar" được chia sẻ trong một số nhóm Zalo, Facebook, Telegram... Khi người dùng tải và giải nén, mã độc sẽ tự động cài vào máy, đánh cắp thông tin đăng nhập Zalo, Facebook, Gmail, ngân hàng, … Đồng thời, mã độc tự động gửi tập tin tương tự để lây lan sang máy tính, thiết bị người dùng khác.

1. Kết quả phân tích về mã độc "DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.exe":

- Kết quả phân tích sơ bộ: Thuộc dòng mã độc Valley RAT.
- Địa chỉ máy chủ điều khiển (C2): 27[.]124[.]9[.]13, port 5689.
- Sự nguy hiểm: Mã độc Valley RAT là một loại Remote Access Trojan (RAT) được phát hiện đầu năm 2023, chủ yếu tấn công người dùng qua các chiến dịch phishing (lừa nạn nhân tải tài liệu mồi nhử có chứa mã độc). Mục đích của ValleyRAT là giám sát và kiểm soát hệ thống bị nhiễm, từ đó tải thêm các plugin độc hại khác để gây hại sâu hơn. Đây là mã độc đa giai đoạn và đa thành phần, có khả năng tránh bị phát hiện bằng cách tải các thành phần theo từng giai đoạn.

2. Các tập tin mã độc khác có kết nối đến địa chỉ máy chủ điều khiển (C2) nói trên mà tin tặc đã phát tán trong thời gian gần đây:

(1) BÁO CÁO TÀI CHÍNH2.exe hoặc THANH TOÁN BẢO HIỂM DOANH NGHIỆP.exe

(2) CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.exe

(3) HỖ TRỢ KÊ KHAI THUẾ.exe

(4) CÔNG VĂN ĐÁNH GIÁ HOẠT ĐỘNG ĐẢNG.exe hoặc MẪU GIẤY ỦY QUYỀN.exe

(5) BIÊN BẢN BÁO CÁO QUÝ III.exe

3. Từ tình hình trên, để ứng phó với sự nguy hiểm và lây lan nhanh chóng của mã độc, Công an tỉnh đề nghị các đơn vị thực hiện một số nội dung sau:

- Nhanh chóng rà soát trong hệ thống thông tin của đơn vị các tập tin nghi ngờ nói trên. Khi ghi nhận sự cố tại đơn vị, đề nghị cách ly máy tính bị nhiễm,

ngắt kết nối Internet, báo cáo tình trạng cụ thể về Công an tỉnh hoặc Trung tâm An ninh mạng Quốc gia, trực thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao – Bộ Công an để được hỗ trợ.

- Quét toàn bộ hệ thống bằng phần mềm bảo mật cập nhật mới nhất (EDR/XDR) có khả năng phát hiện và diệt mã độc ẩn trong bộ nhớ, các driver độc hại. Các giải pháp khuyến nghị trong trường hợp này: Avast bản miễn phí, AVG bản miễn phí, Bitdefender bản miễn phí, Windows Defender bản cập nhật mới nhất. Lưu ý: Kaspersky bản miễn phí chưa phát hiện được mã độc này.

- Trong trường hợp rà quét thủ công: (1) Kiểm tra trên Process Explorer, nếu phát hiện dấu hiệu tiến trình không có chữ ký số, xuất hiện tên tiến trình giả mạo tên tập tin văn bản; (2) Kiểm tra bằng TcpView để xem kết nối mạng nếu phát hiện kết nối về IP máy chủ 27[.]124[.]9[.]13 thì đó chính là mã độc.

- Quản trị viên khẩn trương block trên tường lửa, ngăn chặn truy cập đến địa chỉ IP độc hại: 27[.]124[.]9[.]13.

- Khuyến cáo toàn bộ cán bộ, công chức, viên chức không tải, không mở file ".rar", ".zip" lạ, đặc biệt nếu bên trong có file ".exe" hoặc ".bat"; chỉ nhận tài liệu từ nguồn chính thống, hệ thống nội bộ hoặc đối với người xác thực được; nếu phát hiện hoặc nghi bị nhiễm mã độc, khẩn trương đổi mật khẩu các tài khoản quan trọng (Zalo, Gmail, ngân hàng...).

Công an tỉnh thông báo các đơn vị biết, phối hợp thực hiện./.

Nơi nhận:
- Như kính gửi;
- Đ/c Bí thư Tỉnh ủy (để báo cáo);
- Đ/c Chủ tịch UBND tỉnh (để báo cáo);
- Giám đốc Công an tỉnh (để báo cáo);
- Lưu: VT, PA05(Đ2).C.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH GIA LAI

Đại tá Nguyễn Chí Linh