BỘ CÔNG AN
CÔNG AN TỈNH THANH HÓA

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

Số: 4487 /CAT-ANM&PCTPSDCNC

Thanh Hoá, ngày 10 tháng 11 năm 2025

V/v phòng ngừa, phát hiện và ứng phó mã độc Valley RAT lây nhiễm trong hệ thống thông tin

Kính gửi:
- Văn phòng Tỉnh uỷ;
- Các ban của Tỉnh uỷ;
- Các sở, ban, ngành, đơn vị cấp tỉnh;
- MTTQ và các đoàn thể cấp tỉnh;
- Các đơn vị Trung ương đóng trên địa bàn tỉnh;
- Đảng uỷ, UBND các xã, phường trong tỉnh.

Qua công tác bảo đảm an toàn thông tin, Công an tỉnh phát hiện thời gian gần đây, hoạt động phán tán mã độc qua mạng xã hội (Facebook, Zalo, Telegram) diễn biến phức tạp, tinh vi và hướng đến các cơ quan, đơn vị trong hệ thống chính trị. Đối tượng tấn công thường giả mạo người quen, gửi tệp tin đính kèm hoặc đường dẫn chứa mã độc, dụ người dùng kích hoạt hoặc gửi các tập tin mã độc được đặt tên dưới dạng tài liệu tham khảo vào các nhóm chung nhiều thành viên. Khi nạn nhân mở tệp hoặc truy cập liên kết, thiết bị bị chiếm quyền điều khiển, đánh cắp thông tin đăng nhập, dữ liệu cá nhân, tài khoản ngân hàng hoặc truy cập trái phép vào hệ thống mạng nội bộ của cơ quan, đơn vị.

Cụ thể, Công an tỉnh đã phát hiện tình trạng lây nhiễm mã độc qua các nhóm Zalo chung về chuyển đổi số, học tập nghị quyết, hướng dẫn nghiệp vụ. Đối tượng đặt tên tập tin mã độc dưới dạng tài liệu tham khảo như "DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.rar", "CÔNG VĂN ĐÁNH GIÁ HOẠT ĐỘNG ĐẢNG.rar", "BÁO CÁO TÀI CHÍNH.rar", "THANH TOÁN BẢO HIỂM DOANH NGHIỆP.rar", "CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.rar", "MẪU GIẤY ỦY QUYỀN.rar", "HỖ TRỢ KÊ KHAI THUẾ.rar", "BIÊN BẢN BÁO CÁO QUÝ III.rar". Qua phân tích, đây là dạng 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 Valley RAT là giám sát và kiểm soát hệ thống bị nhiễm, từ đó tải thêm các plugin độc hại khác để gây hại sâu hơn, đánh cắp thông tin, dữ liệu cá nhân. 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. Sau đó, mã độc có thể chiếm quyền các tài khoản mạng xã hội của người dùng và gửi tập tin mã độc đến các nhóm mạng xã hội mà người dùng tham gia để lây nhiễm.

Để tăng cường phòng chống mã độc, đảm bảo an toàn thông tin, Công an tỉnh đề nghị các đơn vị triển khai nghiêm túc các nội dung sau:

1. Tăng cường tuyên truyền, nâng cao nhận thức cho cán bộ, công chức, viên chức, người lao động về nguy cơ mã độc phát tán qua mạng xã hội: Không mở, tải hoặc giải nén các tập tin, đường dẫn lạ được gửi qua Zalo, Facebook, Telegram, email, đặc biệt các tập tin lạ có đuôi ".exe", ".scr", ".bat", ".cmd, ".dll"; không tải phần mềm, tài liệu, công cụ "crack" từ các trang web không rõ nguồn gốc; kiểm tra kỹ tên miền, đường dẫn; không đăng nhập tài khoản cơ quan trên các trang web không chính thống; không lưu mật khẩu trên trình duyệt để đăng nhập tự động…

2. Thực hiện kiểm tra, quét mã độc định kỳ trên máy tính, máy chủ bằng phần mềm diệt virus có bản quyền. Thường xuyên cập nhật bản vá bảo mật cho hệ điều hành, trình duyệt, bộ Office và phần mềm làm việc.

3. Kiểm tra, quét virus các thiết bị ngoại vi (USB, ổ cứng di động…) trước khi kết nối. Tắt tính năng tự động chạy (Autorun) trên máy tính để ngăn mã độc lây qua USB.

4. Rà soát trong hệ thống thông tin các tập tin nghi ngờ mã độc nói trên. Khi phát hiện sự cố lây nhiễm mã độc 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 (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để được hỗ trợ. Triển khai 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 và các driver độc hại. Các phần mềm diệt virus khuyến nghị đối với mã độc Valley RAT: Avast bản miễn phí, AVG bản miễn phí, Bitdefender bản miễn phí, Windows Defender bản cập nhật mới nhất. Phần mềm diệt virus Kaspersky bản miễn phí chưa phát hiện được mã độc này.

Công an tỉnh phân công đồng chí Trung uý Nguyễn Tuấn Anh, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Công an tỉnh (SĐT: 089.863.4198) làm đầu mối liên hệ trao đổi, phối hợp.

Công an tỉnh trao đổi để các đơn vị thực hiện./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc Công an tỉnh;
- Đ/c Đại tá Lê Ngọc Anh – PGĐ CAT;
- Phòng Tham mưu, Công an tỉnh;
- Lưu: VT, ANM&PCTPSDCNC(Đ2).

TL. GIÁM ĐỐC
TRƯỞNG PHÒNG AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO

Thượng tá Nguyễn Quang Thuỷ