CẢNH BÁO KHẨN PHÁT HIỆN MÃ ĐỘC NGUY HIỂM GIẢ MẠO VĂN BẢN CƠ QUAN NHÀ NƯỚC

Mẫu mã độc được ngụy trang dưới dạng tệp tin văn bản có tên “DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.exe”.

🔍 KẾT QUẢ PHÂN TÍCH SƠ BỘ:

Loại mã độc: Valley RAT (Remote Access Trojan). Đây là loại mã độc cho phép tin tặc chiếm quyền điều khiển máy tính của bạn từ xa, theo dõi mọi hoạt động, đánh cắp dữ liệu (tài khoản ngân hàng, tài liệu nội bộ, thông tin cá nhân) và cài đặt thêm các phần mềm độc hại khác.

Địa chỉ máy chủ điều khiển (C2): 27[.]124[.]9[.]13 (Port: 5689)

⚠️ ĐẶC BIỆT NGUY HIỂM: Tin tặc không chỉ sử dụng một tên tệp duy nhất mà liên tục thay đổi tên ngụy trang để lừa người dùng. Cần hết sức cảnh giác với các tệp tin có đuôi ".exe" nhưng có tên gọi giống như tài liệu hành chính, báo cáo, tài chính như:

BÁO CÁO TÀI CHÍNH2.exe

THANH TOÁN BẢO HIỂM DOANH NGHIỆP.exe

CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.exe

HỖ TRỢ KÊ KHAI THUẾ.exe

CÔNG VĂN ĐÁNH GIÁ HOẠT ĐỘNG ĐẢNG.exe

MẪU GIẤY ỦY QUYỀN.exe

BIÊN BẢN BÁO CÁO QUÝ III.exe

🛡️ HƯỚNG DẪN PHÒNG NGỪA VÀ XỬ LÝ KHẨN CẤP 🛡️

1️⃣ Đối với Cán bộ, người dân:

TUYỆT ĐỐI KHÔNG mở các tệp tin có đuôi .exe được gửi qua Email, Zalo, Messenger nếu không chắc chắn 100% về nguồn gốc. Luôn cẩn trọng với các tệp có tên gọi mập mờ, gây tò mò.

Nếu nghi ngờ máy tính bị nhiễm, hãy ngay lập tức ngắt kết nối mạng Internet để ngăn chặn tin tặc điều khiển và đánh cắp dữ liệu.

Sử dụng các phần mềm diệt virus uy tín và cập nhật bản mới nhất để quét toàn bộ máy tính. Các phần mềm miễn phí được khuyến nghị có khả năng phát hiện tốt mã độc này: Avast Free, AVG Free, Bitdefender Free, Windows Defender (cập nhật mới nhất).

Lưu ý: Phiên bản Kaspersky Free hiện chưa nhận diện được mẫu mã độc này.

2️⃣ Đối với Quản trị viên hệ thống tại các cơ quan, đơn vị:

Khẩn trương rà soát hệ thống, tìm kiếm các tệp tin có tên như trên.

Chặn (block) ngay lập tức địa chỉ IP điều khiển mã độc trên tường lửa (Firewall) của đơn vị: 27[.]124[.]9[.]13.

Sử dụng các công cụ chuyên dụng (như Process Explorer, TCPView) để kiểm tra các tiến trình lạ, không có chữ ký số và các kết nối mạng bất thường đến địa chỉ IP nói trên.

Thông báo và yêu cầu toàn bộ người dùng trong đơn vị nâng cao cảnh giác.