UBND TỈNH HÀ TĨNH **SỞ NGOẠI VỤ**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 868 /SNgV-VP V/v đảm bảo an ninh mạng hệ thống thông tin	*Hà Tĩnh, ngày 01 tháng 6 năm 2026*

Kính gửi: Phòng chuyên môn và đơn vị thuộc Sở

Ngày 29/5/2026, Công an tỉnh có Văn bản số 2113/CAT-ANM về việc đảm bảo an ninh mạng hệ thống thông tin; Sở Ngoại vụ yêu cầu các phòng, đơn vị tổ chức thực hiện một số nội dung sau:

1. Thực hiện nghiêm túc các quy định pháp luật về bảo vệ bí mật nhà nước, các quy định về quản lý, sử dụng các trang thiết bị máy tính, thiết bị lưu trữ ngoài.

2. Rà soát, bóc gỡ (nếu có) mã độc Mustang Panda tại máy tính của các phòng, đơn vị theo hướng dẫn tại phụ lục kèm theo.

File cài đặt "MustangKiller.exe" được gửi kèm theo văn bản.

Quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc trao đổi qua Văn phòng (đồng chí Trần Thị Thúy) để được hướng dẫn, hỗ trợ.

Đề nghị các phòng, đơn vị triển khai thực hiện nghiêm túc, báo cáo kết quả thực hiện về Văn phòng Sở **trước ngày 10/6/2026**./.

Nơi nhận:
- Như trên;
- Công an tỉnh (để b/c);
- BGĐ Sở;
- Lưu: VT, VP_3.

TL. GIÁM ĐỐC
CHÁNH VĂN PHÒNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ NGOẠI VỤ
TỈNH HÀ TĨNH

Trần Thị Như Ý

PHỤ LỤC

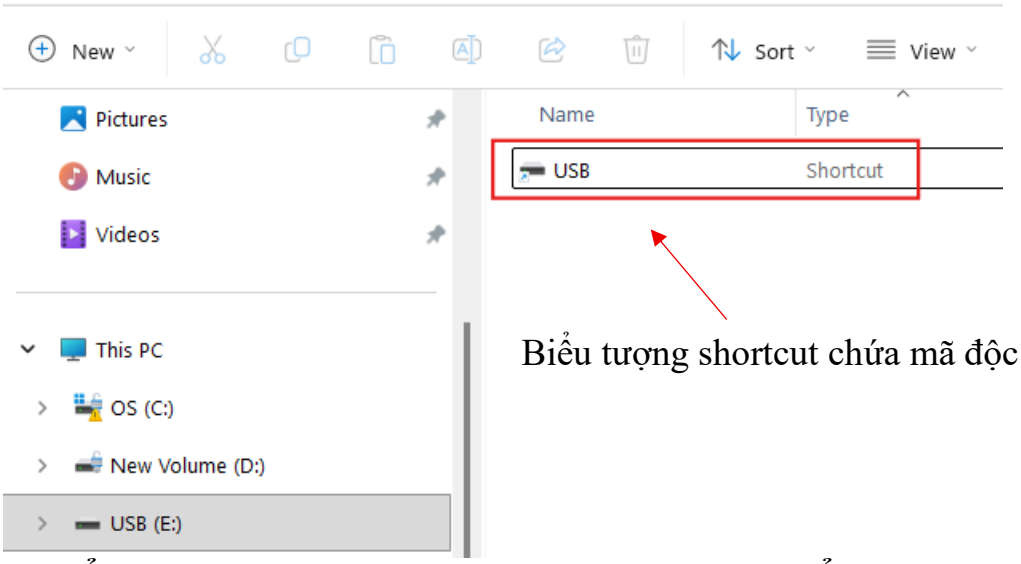
HƯỚNG DẪN PHÁT HIỆN, GỠ BỎ MÃ ĐỘC MUSTANG PANDA

(Kèm theo Văn bản số /SNgV-VP ngày / /2026)

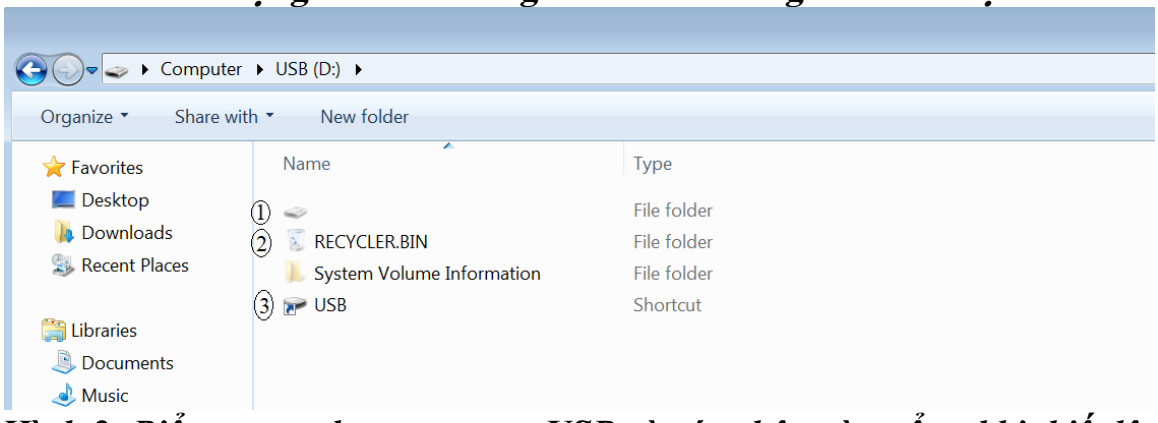
I. Dấu hiệu phát hiện máy tính, thiết bị ngoại vi lây nhiễm mã độc

- Khi sử dụng thiết bị lưu trữ ngoài vào máy tính, toàn bộ dữ liệu trên USB, đĩa CD tự động biến mất, chỉ còn biểu tượng shortcut (*như Hình 1*), người dùng click đúp vào biểu tượng shortcut này sẽ nhìn thấy dữ liệu trên thiết bị cần sao chép.

- Khi sử dụng thiết bị lưu trữ ngoài (USB, thẻ nhớ máy ảnh, CD dạng USB) máy có dấu hiệu hoạt động chậm, ổ đĩa quay nhanh, kêu to bất thường; dung lượng đã sử dụng của USB cao hơn nhiều so với tổng dung lượng file thực tế trên USB.



Hình 1: Biểu tượng shortcut trong USB <khi không cho hiển thị các file ẩn>

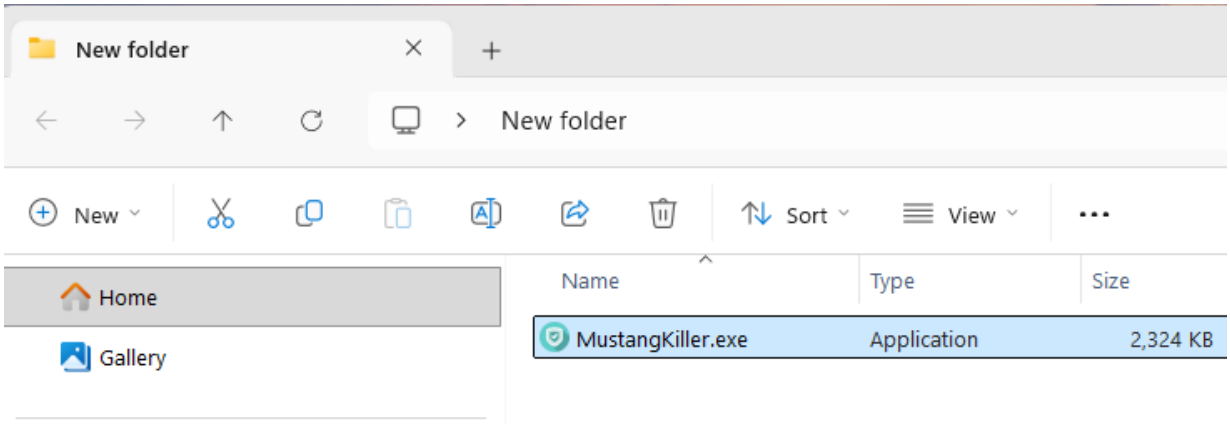


Hình 2: Biểu tượng shortcut trong USB và các phân vùng ẩn <khi thiết lập chức năng hiển thị các file ẩn>

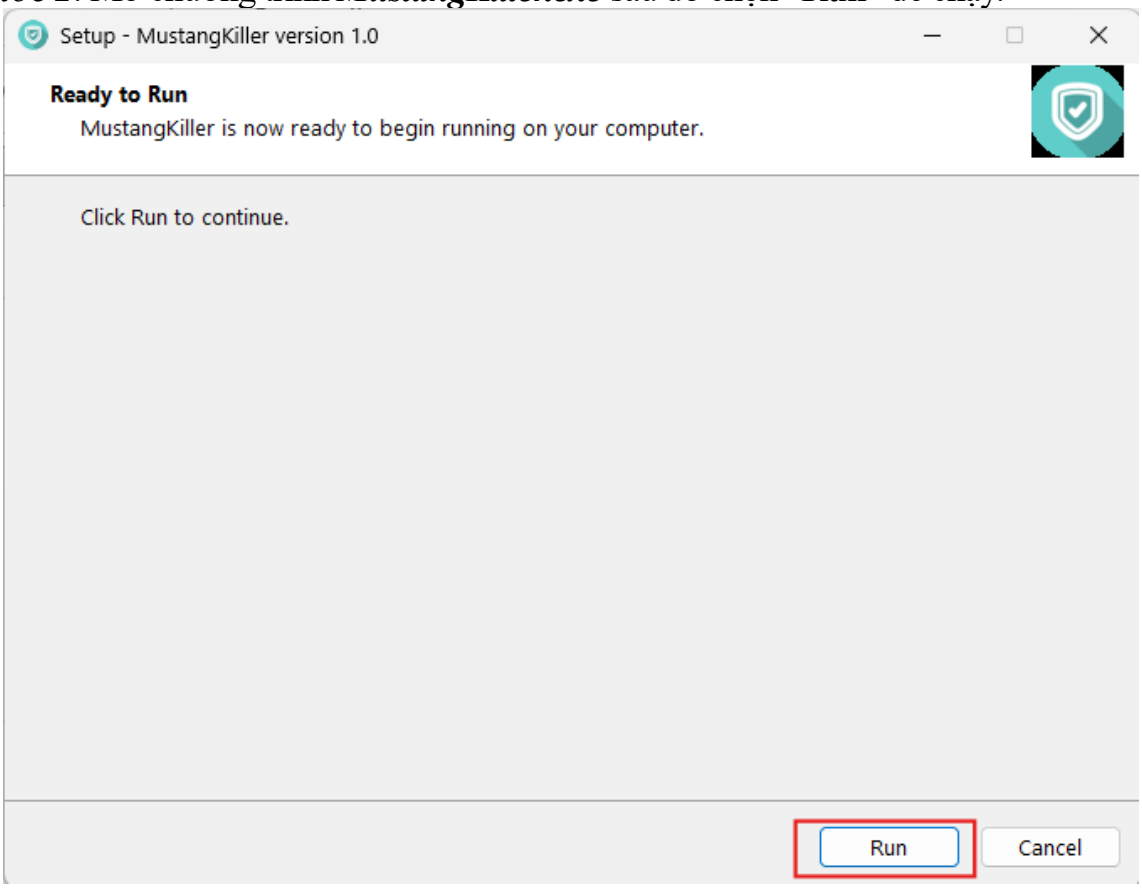
II. Rà quét, bóc gỡ mã độc

Để rà quét, phát hiện mã độc Mustang Panda lây nhiễm trên máy tính, sử dụng công cụ rà quét để phát hiện và gỡ bỏ mã độc (*mã MD5:* 29FD9F3F77687BD23579D584E363DF4B) theo các bước cụ thể như sau:

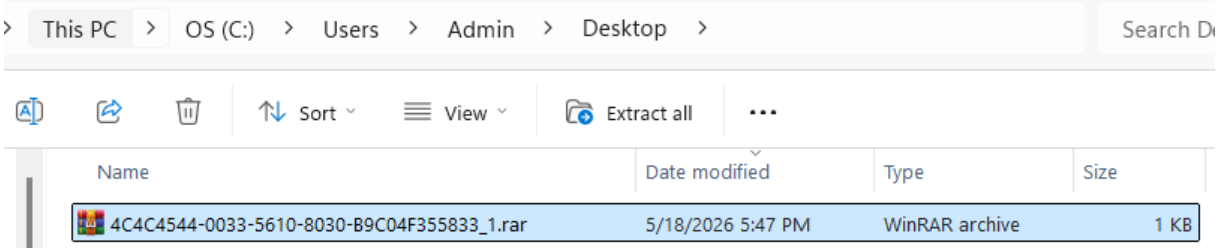
Bước 1: Sử dụng USB (*USB an toàn hoặc USB cơ yếu, lưu ý không sử dụng USB thông thường*) sao chép công cụ ***MustangKiller.exe*** vào máy tính cần thực hiện.



Bước 2: Mở chương trình ***MustangKiller.exe*** sau đó chọn "**Run**" để chạy.



Bước 3: Chương trình sẽ diệt mã độc, xóa các tệp tin độc hại trên máy, xóa autorun, thu thập mẫu mã độc, tập hợp kết quả rà quét vào tệp tin nén có đuôi ***.rar*** đặt ngoài màn hình máy tính người dùng (*như Hình 3*), đồng thời, kết quả rà quét sẽ hiển thị trên màn hình (*như Hình 4*).



Hình 3: Tệp tin nén có đuôi ".rar" chứa kết quả rà quét

Hình 4: Cửa sổ hiển thị kết quả rà quét

Bước 4: Cán bộ thực hiện copy tệp tin kết quả vào USB (*USB an toàn hoặc USB cơ yếu, lưu ý không sử dụng USB thông thường*) để tập hợp kết quả (***lưu ý chỉ chấp nhận tệp tin có đuôi _1.rar***).

Sau khi thực hiện rà quét toàn đơn vị, cán bộ được giao nhiệm vụ triển khai rà quét tập hợp các tệp tin kết quả từ các máy tính của đơn vị mình lưu thành thư mục đặt tên theo tên đơn vị (ví dụ: HaTinh_SoGiaoducvaDaotao; HaTinh_ThanhSen) để tập hợp trao đổi lại cán bộ hướng dẫn trực tiếp của đơn vị cấp trên để tập hợp trao đổi Công an tỉnh qua đầu mối Công văn này. Tập hợp các kết quả sẽ lưu tại 3 nơi: đơn vị được kiểm tra, Công an tỉnh, Cục A05 để đối sánh, thống nhất để kiểm tra.