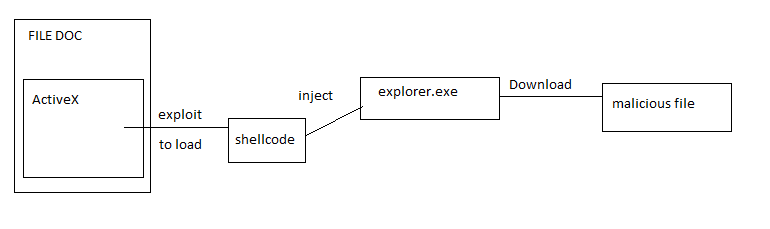
Md5:

Phân loại: Office malware, ActiveX Download

Luồng hoạt động chính



Sử dụng CVE 2018-4878 để exploit ActiveX - Adobe Flash Player nhúng trong file DOC

Khi exploit thành công sẽ chạy shellcode có chứa trong nó

Load các System API:

ntdll.RtlCreateUserThread, ntdll.NtClose

kernel32.OpenProcessStub, kernel32.VirtualAllocExStub, kernel32.WriteProcessMemoryStub, kernel32.VirtualFreeExStub, kernal32.WaitForSingleObject

Sau đó nó inject chính nó vào process Explorer.exe

Đến địa chỉ “falcancoin.io” và download 2 file /data/package32.zip và /data/package64.zip rồi load chúng