











rule unknown\_malware

{

    meta:

        name = "Ayah Elajlouni"

SID = "20180262"

        md5 = "7258DE07AD9C7CCD33ED06E2B45F2B63"

        sha1 = "3D2661DCE8C0F45D67AFF08055098C4B99F58C59"

        sha256="B7463684306CD61455715CAE951EF13C4A40F529F09F21535FEED458DC901708"

    strings:

$MZ={4D 5A}

$s1 = "PSUT.DLL"

        $s2 = "No internet, No game"

$s3 = "VBA6.DLL"

        $s4 = "Unknown\_Malware"

        $s5 = "CaesarCipher"

        $s6 = "This benign malware is wrtten for malware analysis purposes. It causes no harm to your computer"

        $s7 = "<http://www.example.com/post_handler>"

        $s8 = "[https://www.google.com](https://www.google.com/)"

$s9 = "application/x-www-form-urlencoded"

    condition:

        $s1 and $s2 and $s3 and $s4 and $s5 and $s6 and $s7 and $s8 and $s9 and $MZ

}