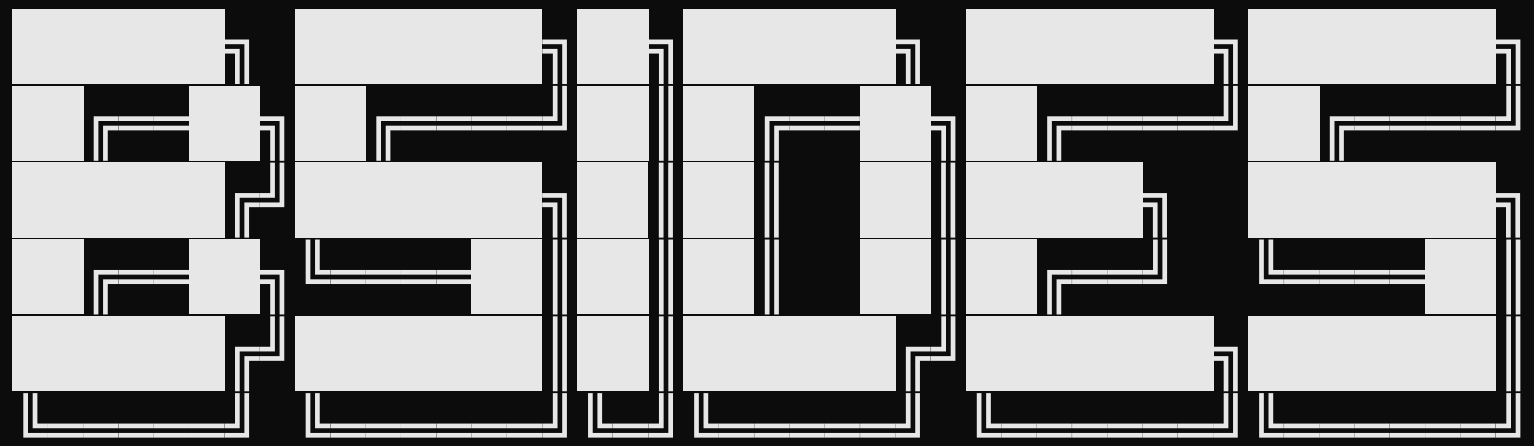
C:\Windows\system32\cmd.e:

C:\>



##

by Bojan Alikavazovic (INFIGO IS)

C:\Windows\system32\cmd.e:

C:\Users\bojan.alikavazovic>

[*] Principal CTI Specialist (INFIGO IS)

> Intelligence Analysis

> Reversing

> Incident Response (support)

> linkedin.com/in/balikavazovic/

C:\Windows\system32\cmd.e:

C:\>type agenda.txt

> ICS and Incident Response

> Window OS - Brief history

> Using CMD for incident scoping


INDUSTRIAL
CONTROL SYSTEMS

C:\Windows\system32\cmd.e:

C:\>type IT_vs_OT.txt

IT	OT
Data protection	Process protection
Unpredictable patterns	Predictable patterns
H. upgr. 3 - 5 yr.	H. upgr. 10 - 15 yr.
Frequent changes	Rare changes
Secure by design	Unsecure by design

C:\Windows\system32\cmd.e:

C:\>type OT.txt

> "Watch - don't touch"
> (If you've been to the museum, it's the same approach.)

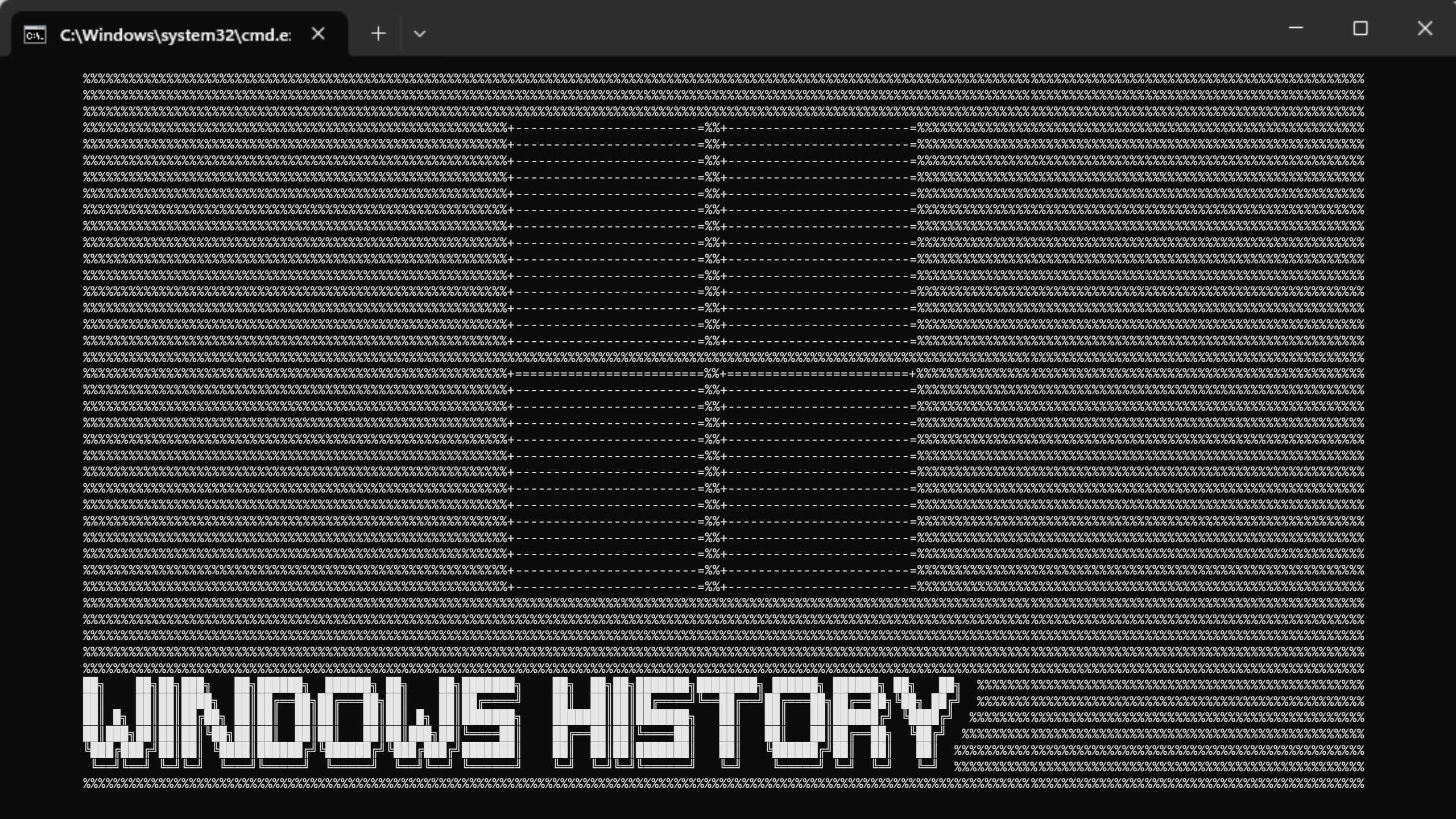
> It's all about availability
> (Uptime is measured in years.)

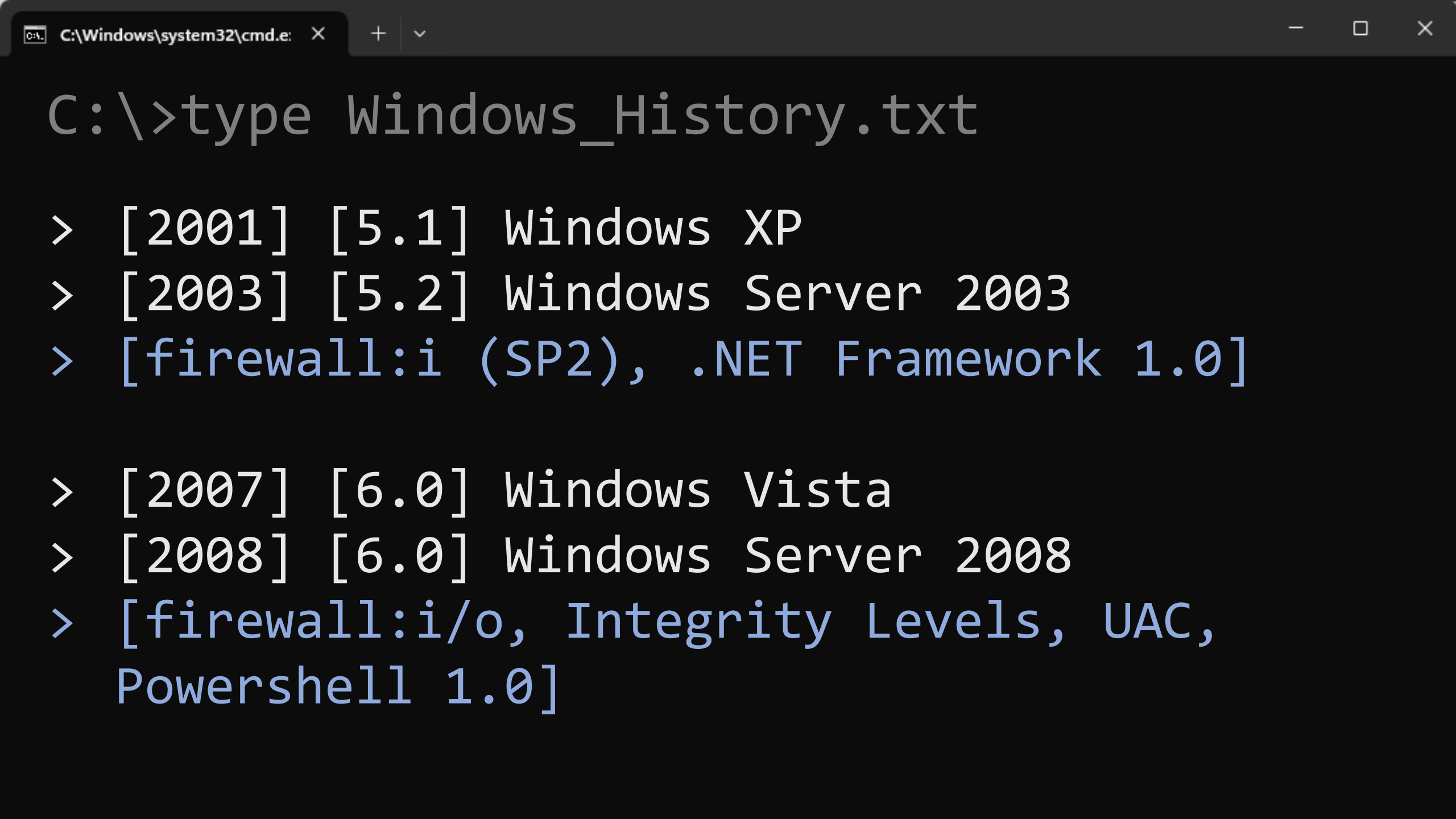
C:\Windows\system32\cmd.e:

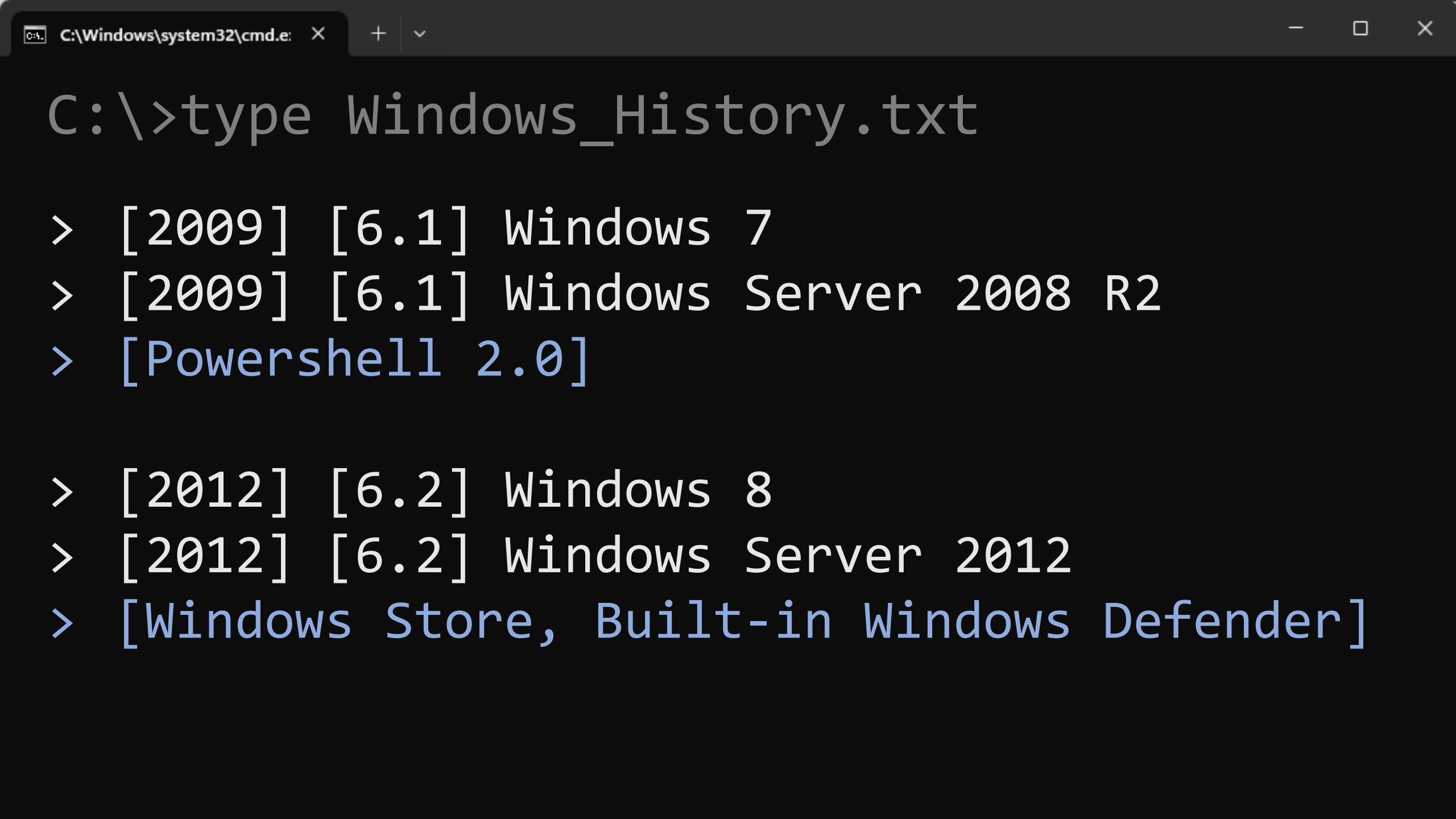
C:\>type IR_Notes.txt

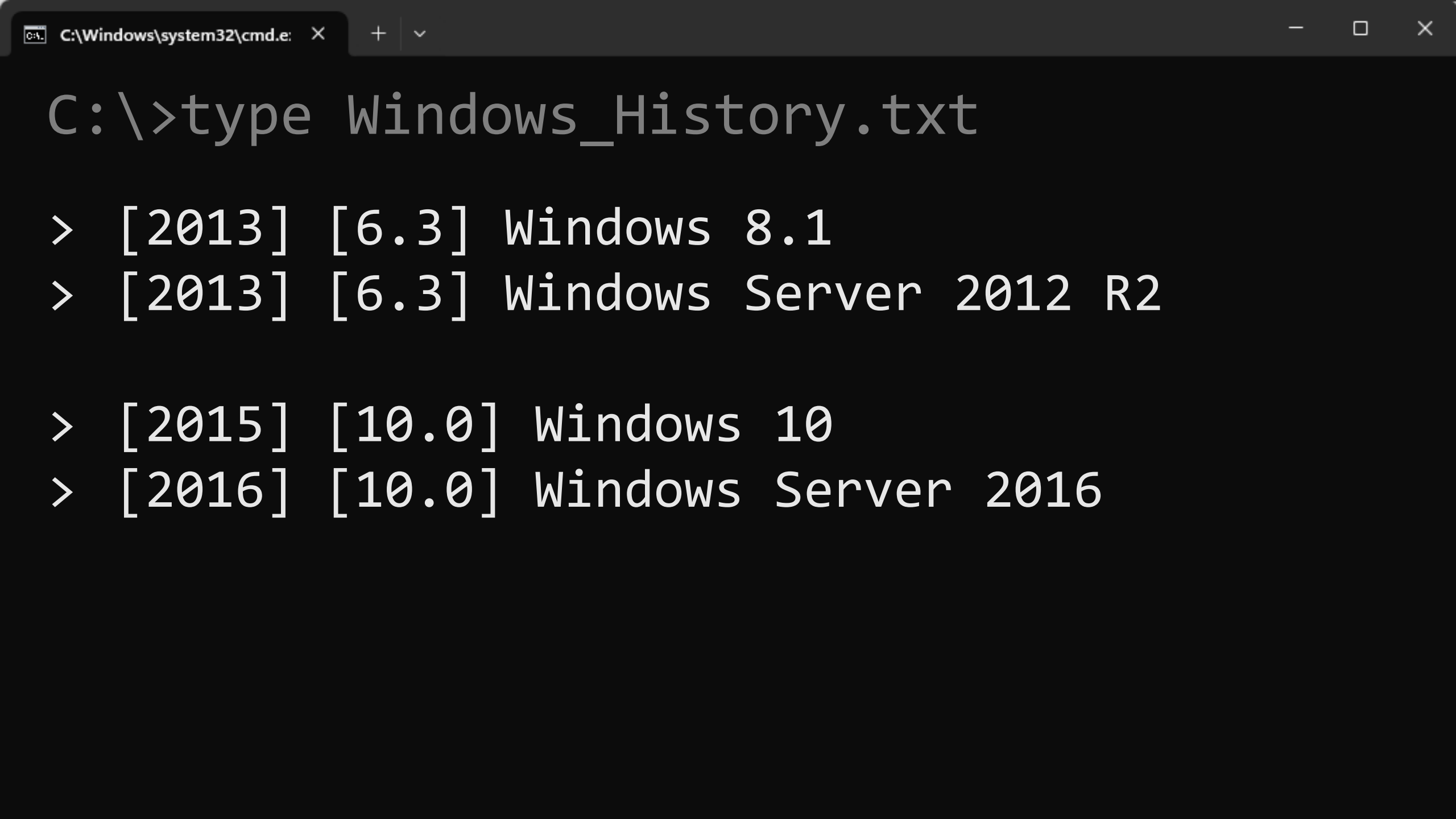
> The computer is infected, what will you do?
> Unplug it? > NO!

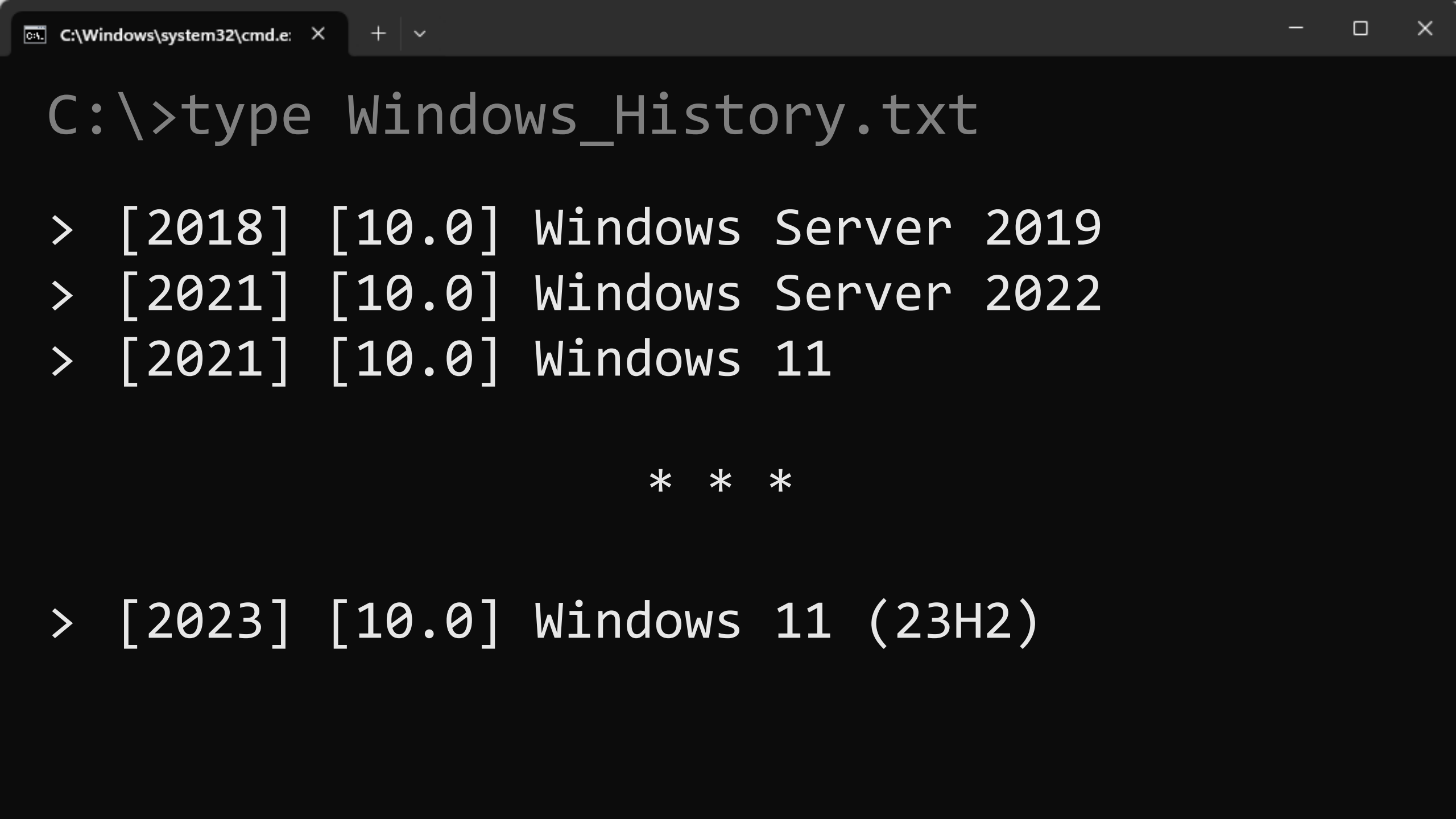
> "Watch - don't touch"
> Talk to the technologists > assess the threat > make a plan > then proceed!


C:\Windows\system32\cmd.e:
WINDOWS HISTORY


C:\Windows\system32\cmd.e:
C:\>type Windows_History.txt
> [2001] [5.1] Windows XP
> [2003] [5.2] Windows Server 2003
> [firewall:i (SP2), .NET Framework 1.0]
> [2007] [6.0] Windows Vista
> [2008] [6.0] Windows Server 2008
> [firewall:i/o, Integrity Levels, UAC,
Powershell 1.0]


C:\Windows\system32\cmd.e:
C:\>type Windows_History.txt
> [2009] [6.1] Windows 7
> [2009] [6.1] Windows Server 2008 R2
> [Powershell 2.0]
> [2012] [6.2] Windows 8
> [2012] [6.2] Windows Server 2012
> [Windows Store, Built-in Windows Defender]


C:\Windows\system32\cmd.e:
C:\>type Windows_History.txt
> [2013] [6.3] Windows 8.1
> [2013] [6.3] Windows Server 2012 R2
> [2015] [10.0] Windows 10
> [2016] [10.0] Windows Server 2016

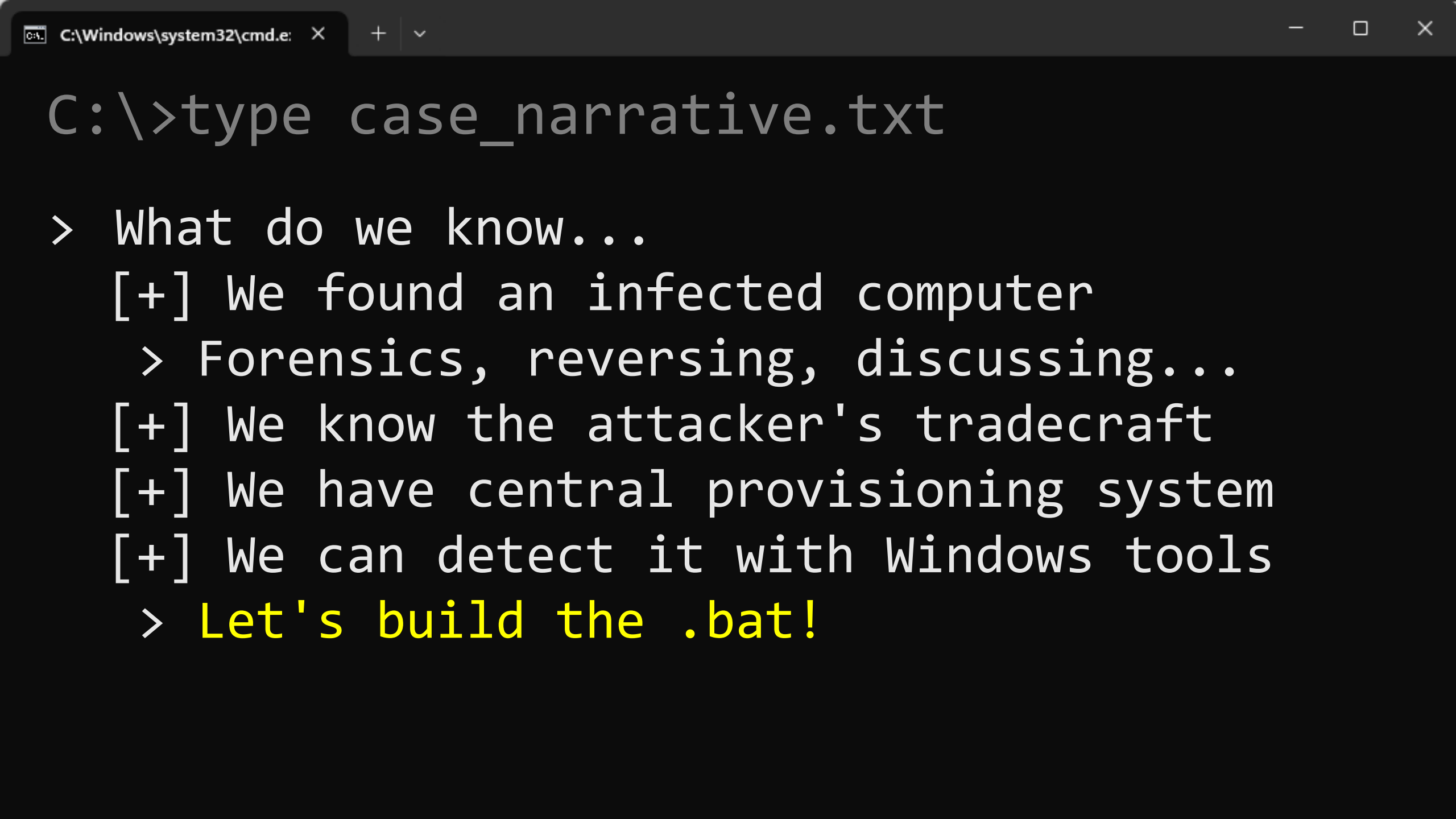

C:\Windows\system32\cmd.e:
C:\>type Windows_History.txt
> [2018] [10.0] Windows Server 2019
> [2021] [10.0] Windows Server 2022
> [2021] [10.0] Windows 11
* * *
> [2023] [10.0] Windows 11 (23H2)


C:\Windows\system32\cmd.e:
CASE: AV DRIVER

C:\Windows\system32\cmd.e:

C:\>type case_narrative.txt

> In the beginning...
  [!] The attacker is in the system
  [!] Several hundred servers in the network
  [!] Different versions of Windows
  [!] Old, unpatched
  [!] Shutting down is not an option
  [!] Installing anything is not an option
  [!] Overloading is not an option (CPU/RAM)

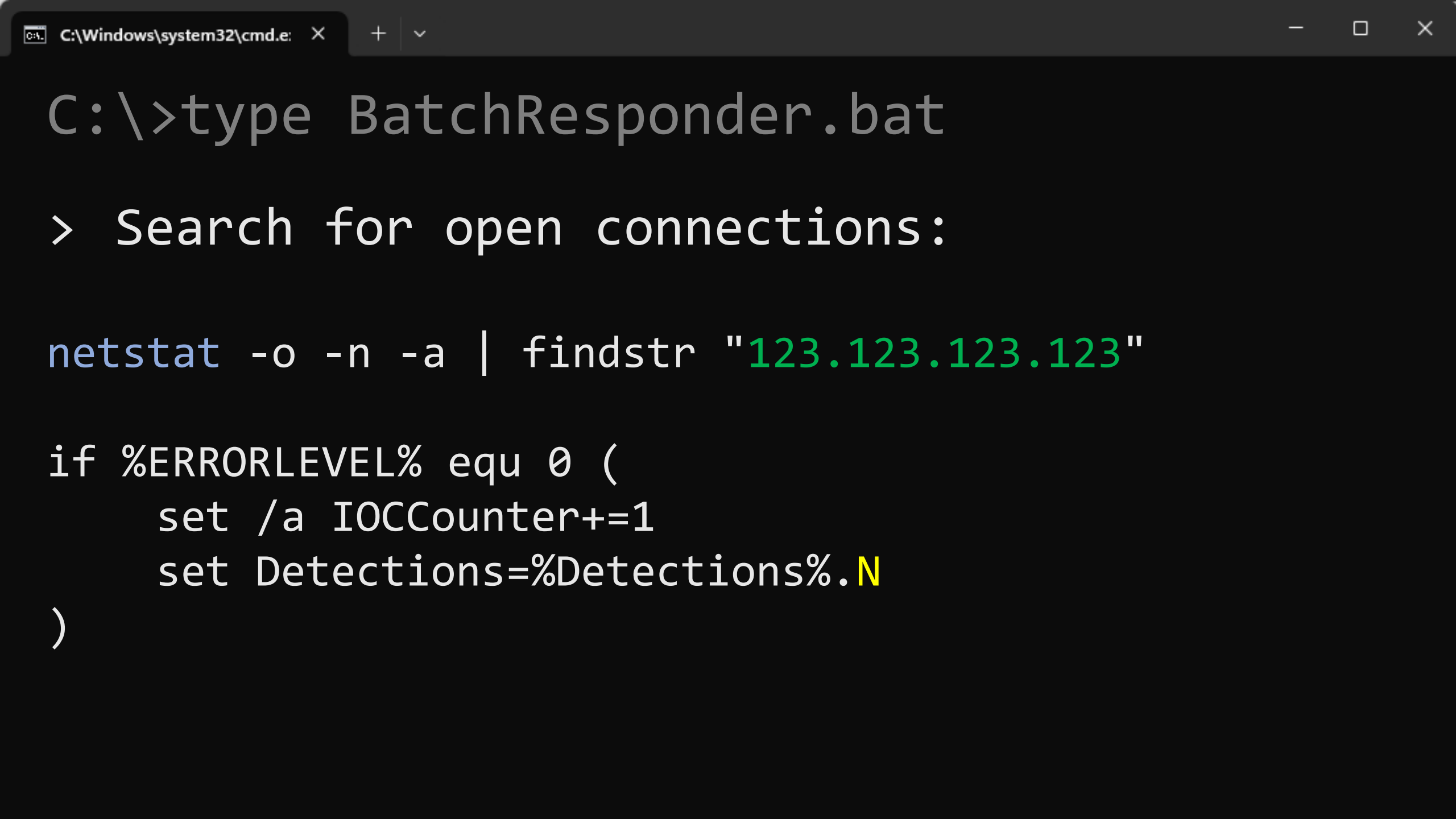

C:\Windows\system32\cmd.e:
C:\>type case_narrative.txt
> What do we know...
[+] We found an infected computer
> Forensics, reversing, discussing...
[+] We know the attacker's tradecraft
[+] We have central provisioning system
[+] We can detect it with Windows tools
> Let's build the .bat!

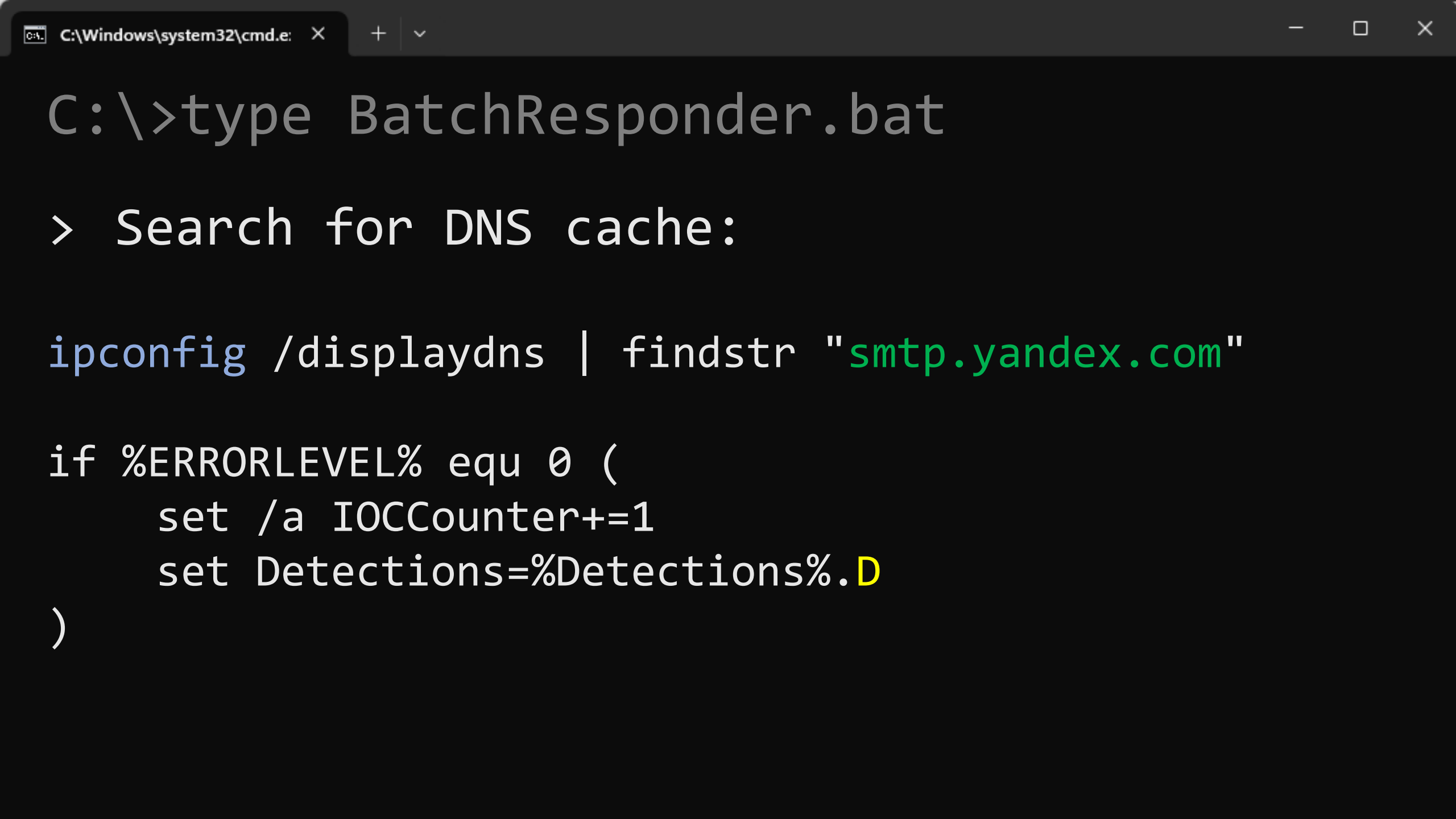
C:\Windows\system32\cmd.e:

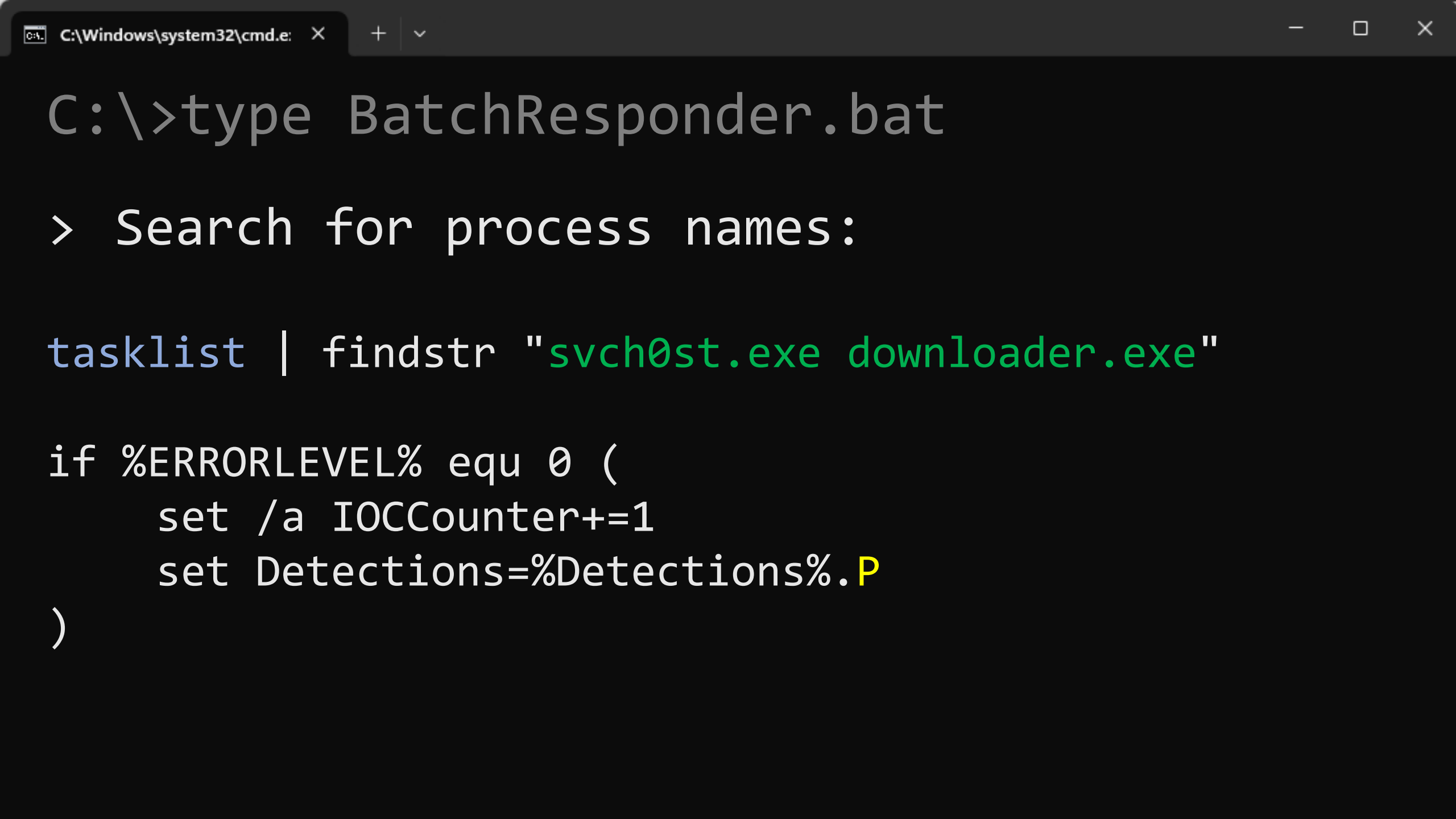
C:\>type BatchResponder.bat

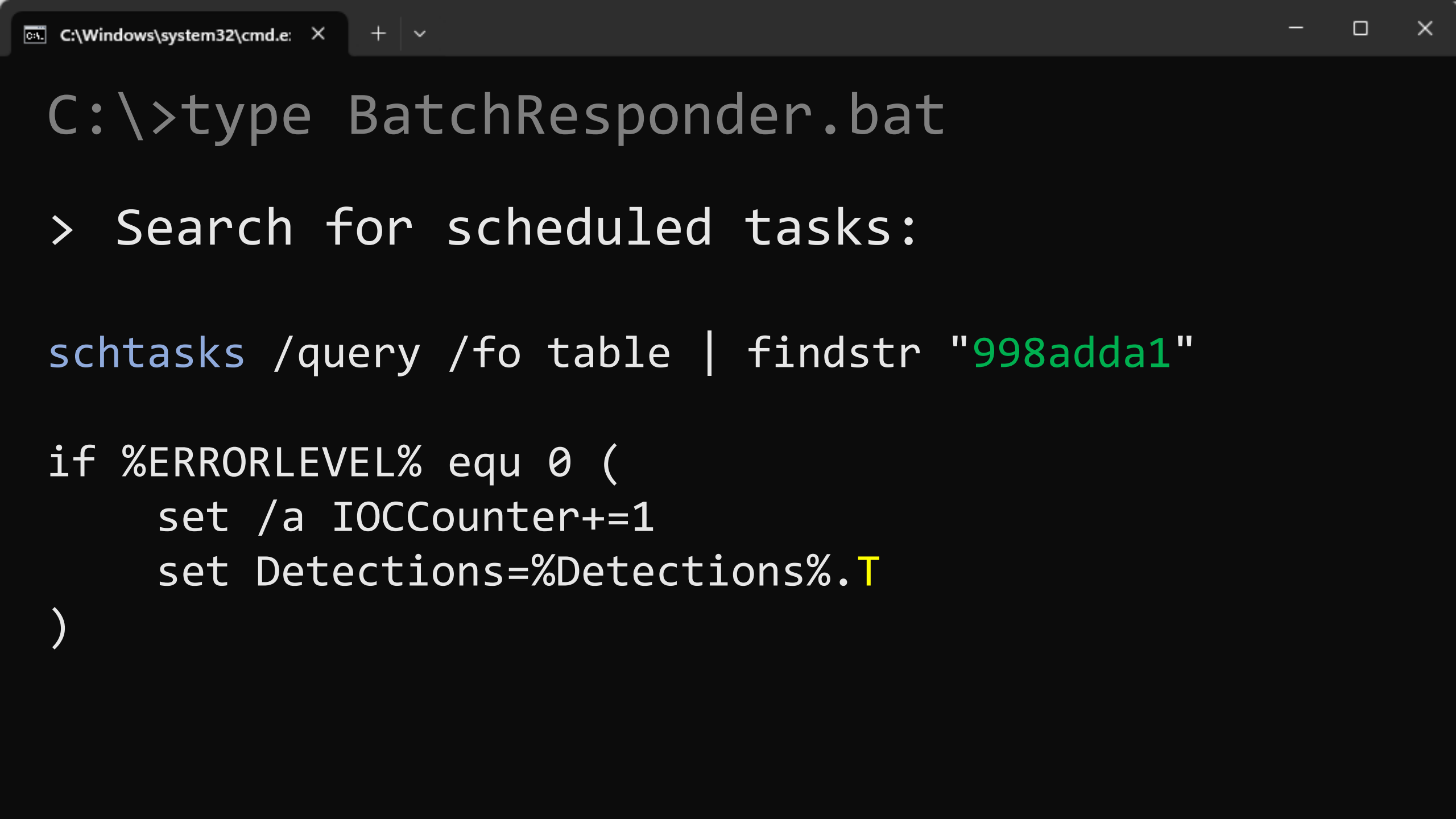
> Search for specific files:

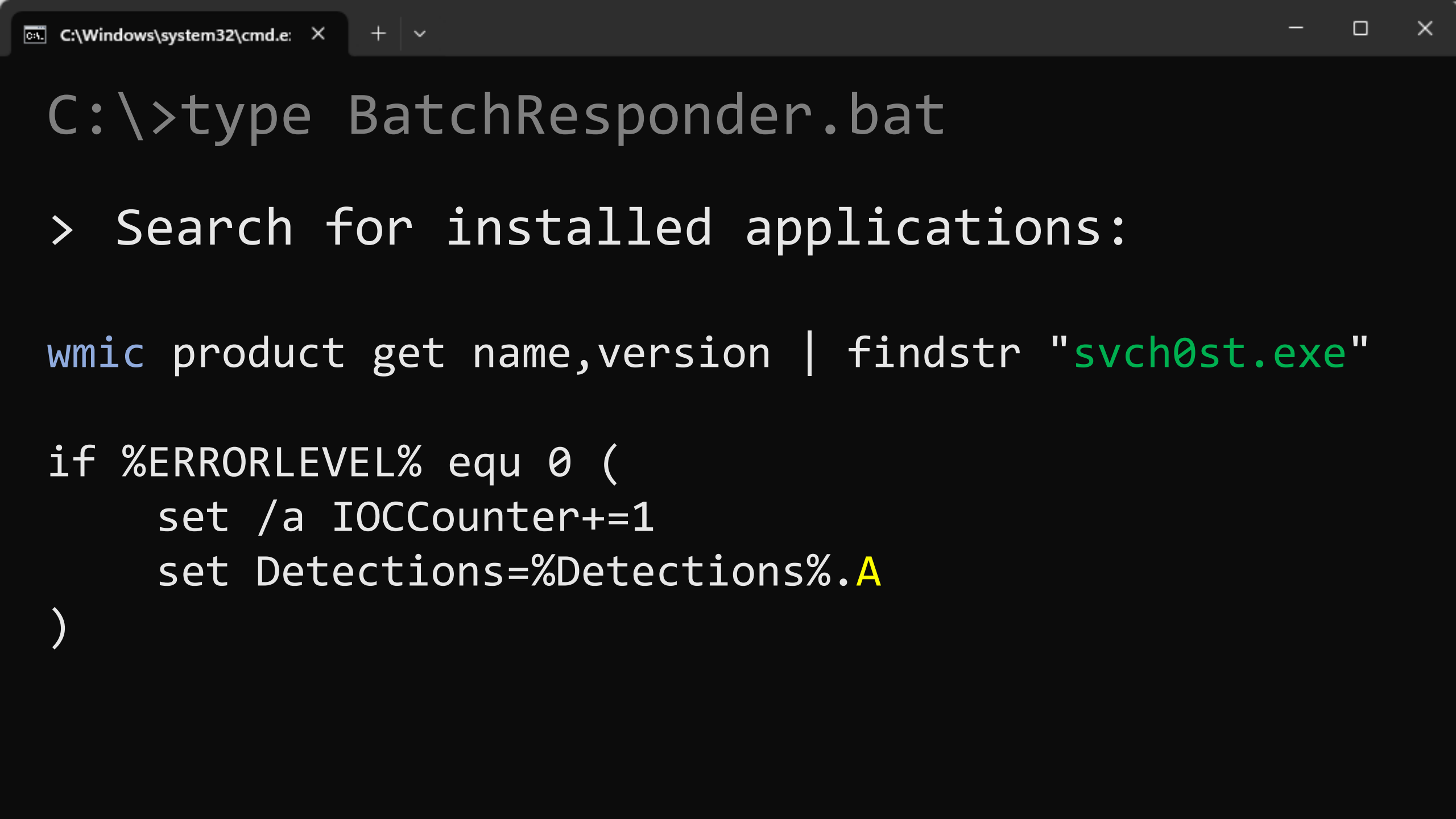
```
for %%F in ("C:\system.vbs %systemroot%\avast.dll")
do (
        if exist "%%F" (
                set /a IOCCounter+=1
                set Detections=%Detections%.F
         )
)
```


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Search for open connections:
netstat -o -n -a | findstr "123.123.123.123"
if %ERRORLEVEL% equ 0 (
set /a IOCCounter+=1
set Detections=%Detections%.N
)


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Search for DNS cache:
ipconfig /displaydns | findstr "smtp.yandex.com"
if %ERRORLEVEL% equ 0 (
set /a IOCCounter+=1
set Detections=%Detections%.D
)


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Search for process names:
tasklist | findstr "svch0st.exe downloader.exe"
if %ERRORLEVEL% equ 0 (
set /a IOCCounter+=1
set Detections=%Detections%.P
)


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Search for scheduled tasks:
schtasks /query /fo table | findstr "998adda1"
if %ERRORLEVEL% equ 0 (
set /a IOCCounter+=1
set Detections=%Detections%.T
)


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Search for installed applications:
wmic product get name,version | findstr "svch0st.exe"
if %ERRORLEVEL% equ 0 (
set /a IOCCounter+=1
set Detections=%Detections%.A
)

C:\Windows\system32\cmd.e:

```
C:\>type BatchResponder.bat

> Search for configured services:

net start | findstr "Windows Update Manager"

if %ERRORLEVEL% equ 0 (
    set /a IOCCounter+=1
    set Detections=%Detections%.S
)
```

C:\Windows\system32\cmd.e:

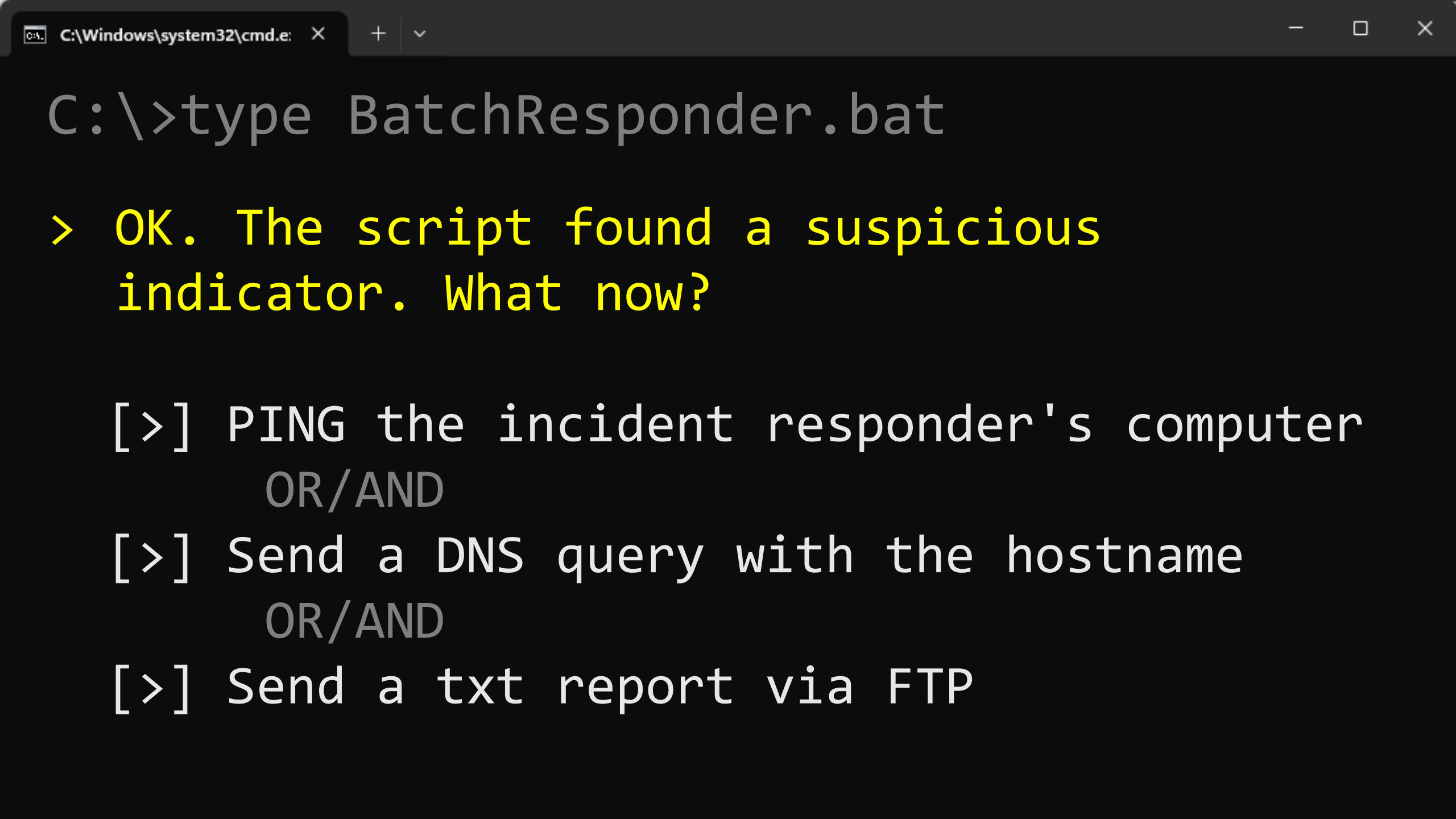
```
C:\>type BatchResponder.bat

> Search for Registry configuration:

reg query
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVers
ion\WindowsUpdate /v Update | findstr "mshta.exe"

if %ERRORLEVEL% equ 0 (
     set /a IOCCounter+=1
     set Detections=%Detections%.R
)
```

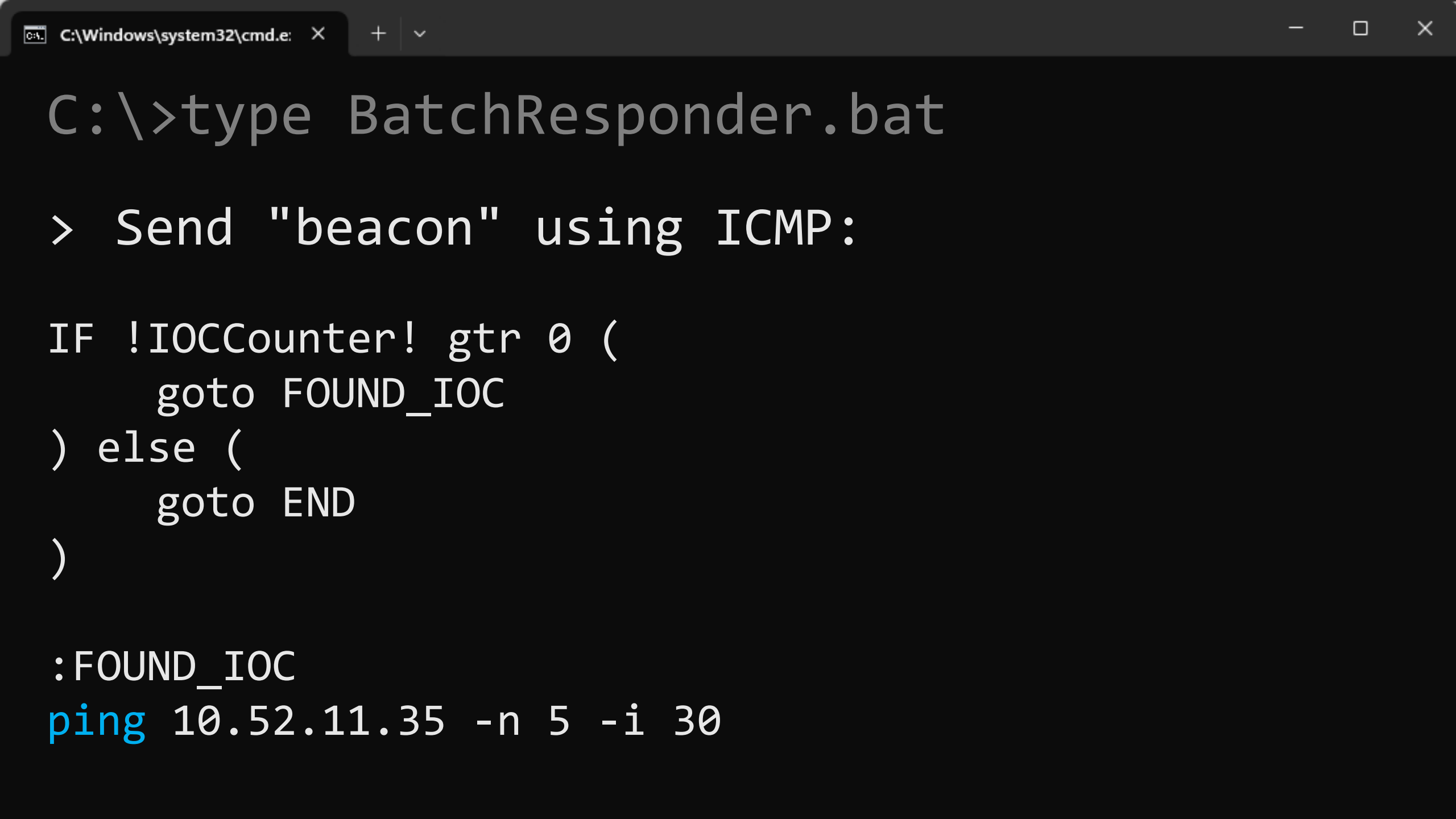
C:\Windows\system32\cmd.e:

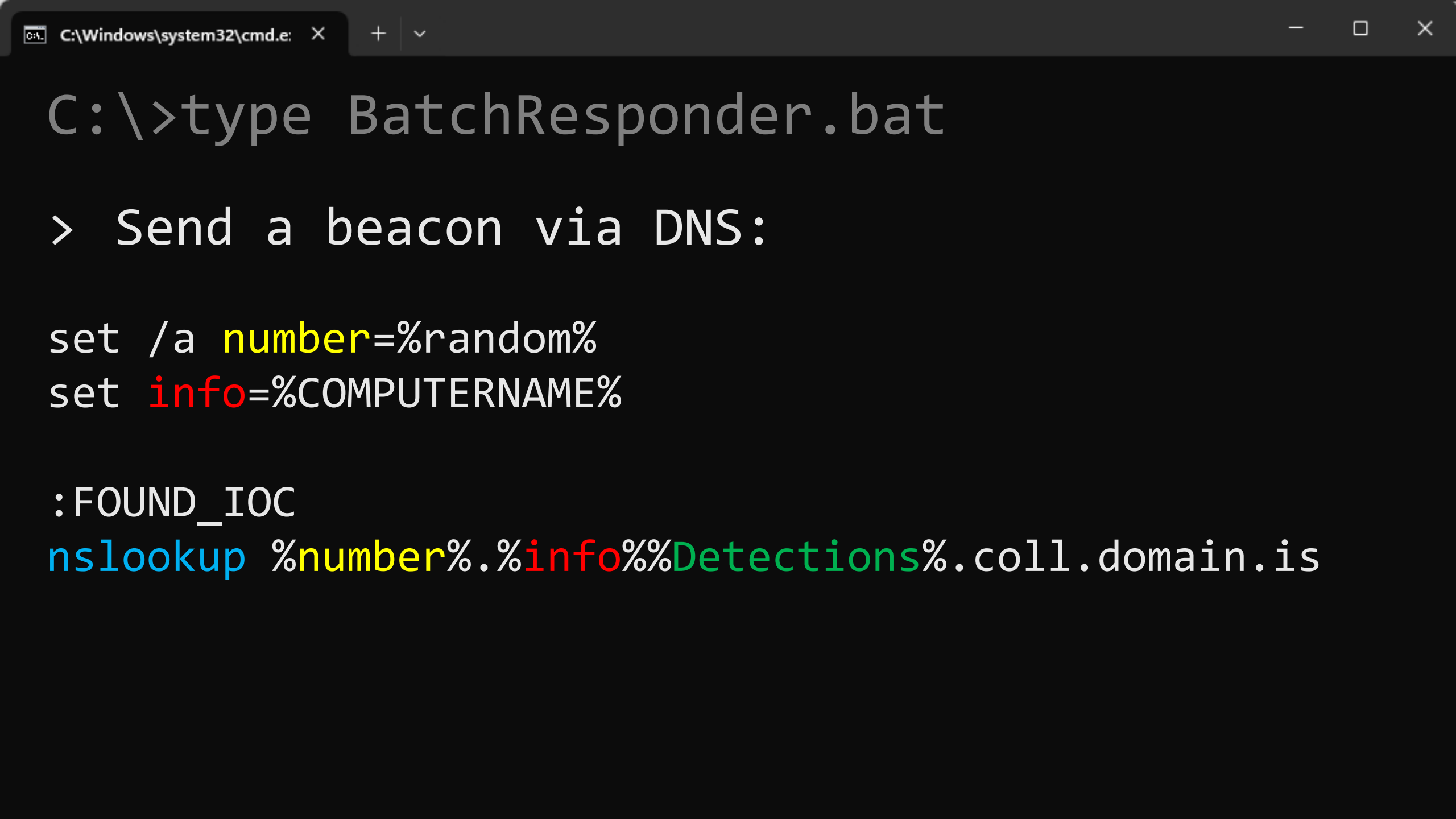
```
C:\>type BatchResponder.bat

> Search for active RDP sessions:

qwinsta | findstr ">rdp" | findstr "newadmin"

if %ERRORLEVEL% equ 0 (
    set /a IOCCounter+=1
    set Detections=%Detections%.E
)
```

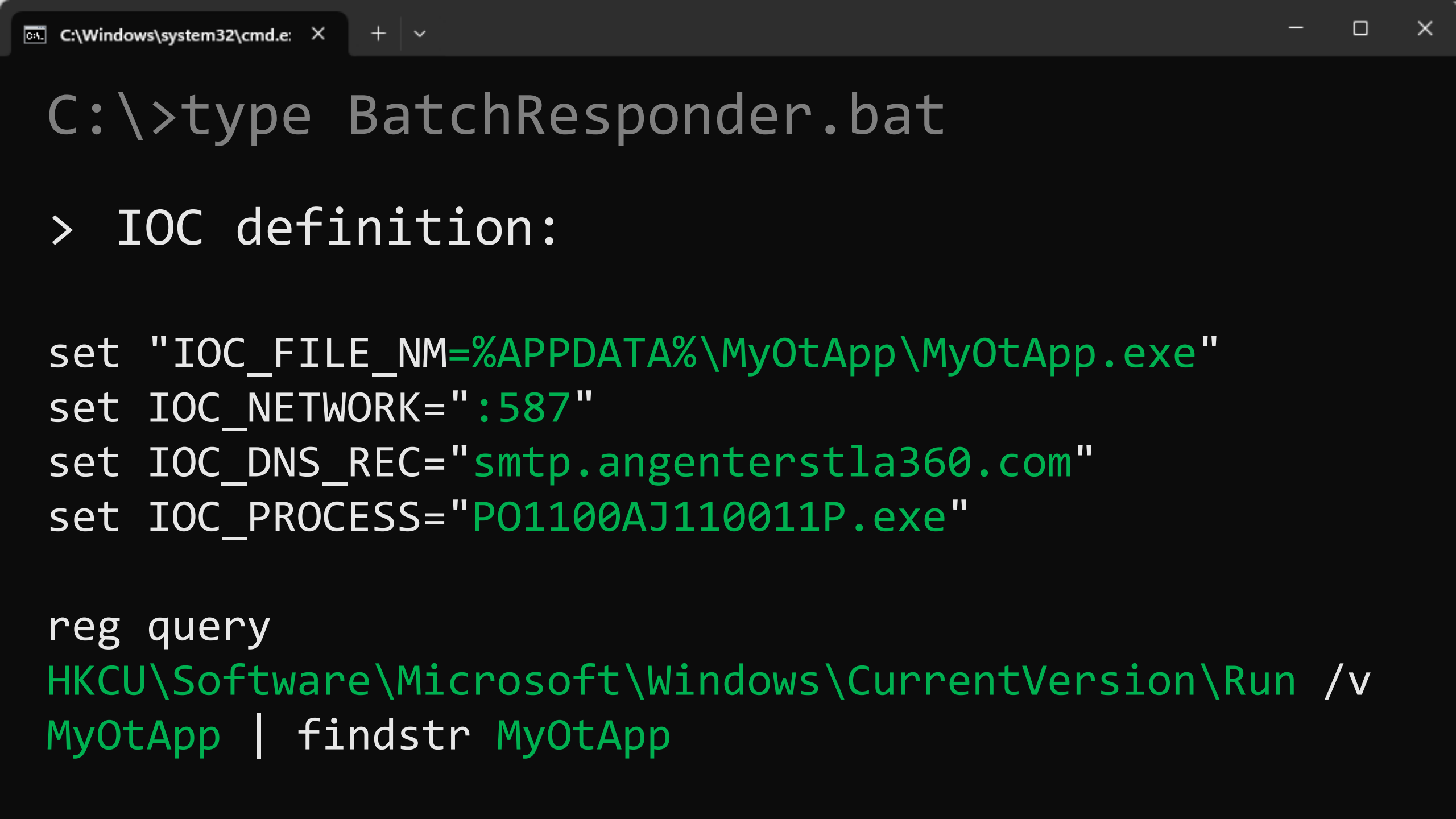
C:\Windows\system32\cmd.e:

```
C:\>type BatchResponder.bat

> Search for user accounts:

net user | findstr "newadmin"

if %ERRORLEVEL% equ 0 (
    set /a IOCCounter+=1
    set Detections=%Detections%.U
)
```

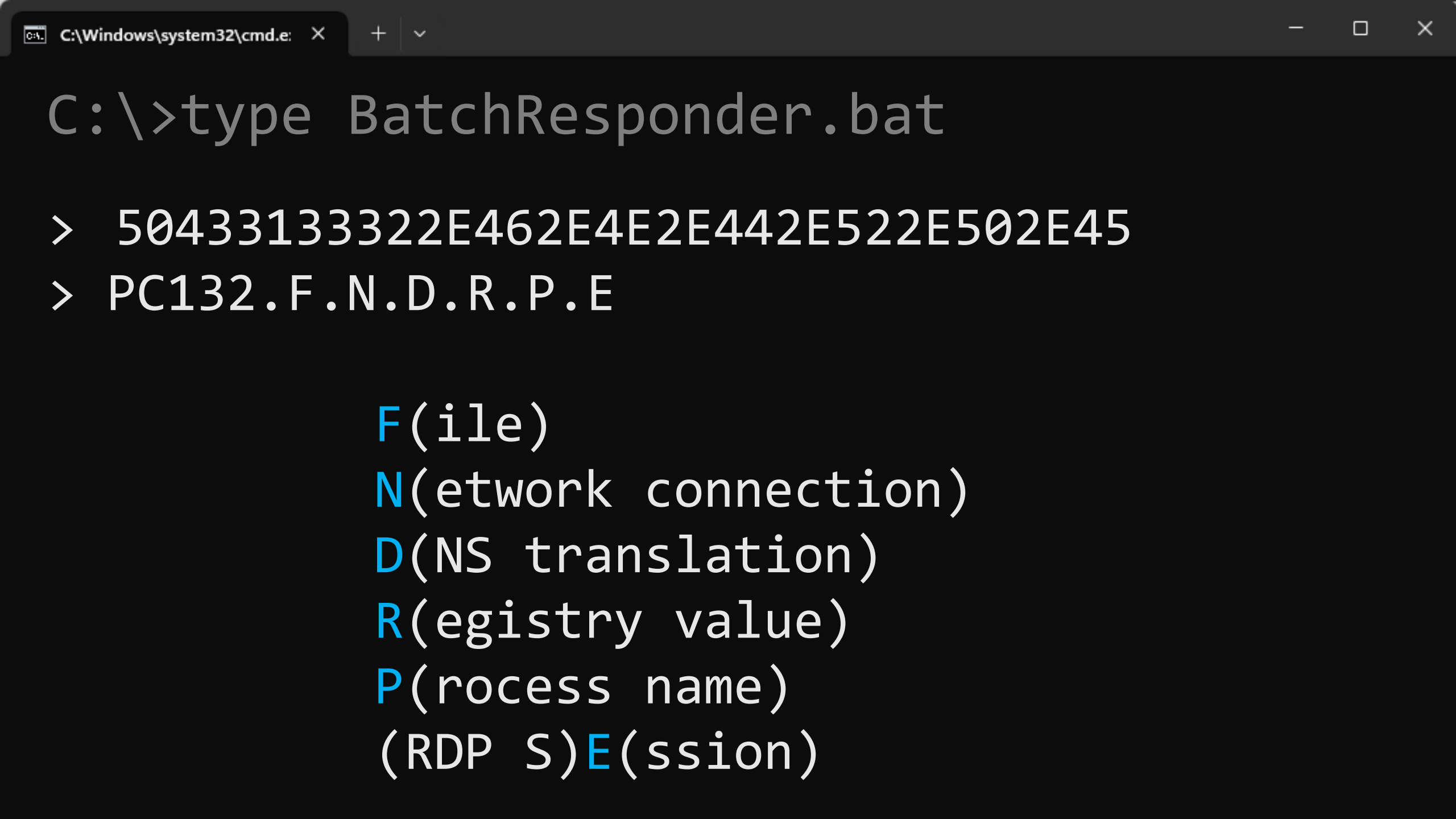

C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> OK. The script found a suspicious indicator. What now?
[>] PING the incident responder's computer
OR/AND
[>] Send a DNS query with the hostname
OR/AND
[>] Send a txt report via FTP


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Send "beacon" using ICMP:
IF !IOCCounter! gtr 0 (
goto FOUND_IOC
) else (
goto END
)
:FOUND_IOC
ping 10.52.11.35 -n 5 -i 30


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> Send a beacon via DNS:
set /a number=%random%
set info=%COMPUTERNAME%
:FOUND_IOC
nslookup %number%.%info%%Detections%.coll.domain.is


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> IOC definition:
set "IOC_FILE_NM=%APPDATA%\MyOtApp\MyOtApp.exe"
set IOC_NETWORK=":587"
set IOC_DNS_REC="smtp.angenterstla360.com"
set IOC_PROCESS="PO1100AJ110011P.exe"
reg query
HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v
MyOtApp | findstr MyOtApp


C:\Windows\system32\cmd.e:
C:\>
DEMO


C:\Windows\system32\cmd.e:
C:\>type BatchResponder.bat
> 50433133322E462E4E2E442E522E502E45
> PC132.F.N.D.R.P.E
F(ile)
N(etwork connection)
D(NS translation)
R(egistry value)
P(rocess name)
(RDP S)E(ssion)

C:\Windows\system32\cmd.e:

```
C:\>start msedge
https://github.com/bojanalikavazovic/BatchResponder
```

C:\Windows\system32\cmd.e:

```
C:\>shutdown -s -t 0 -f
```