

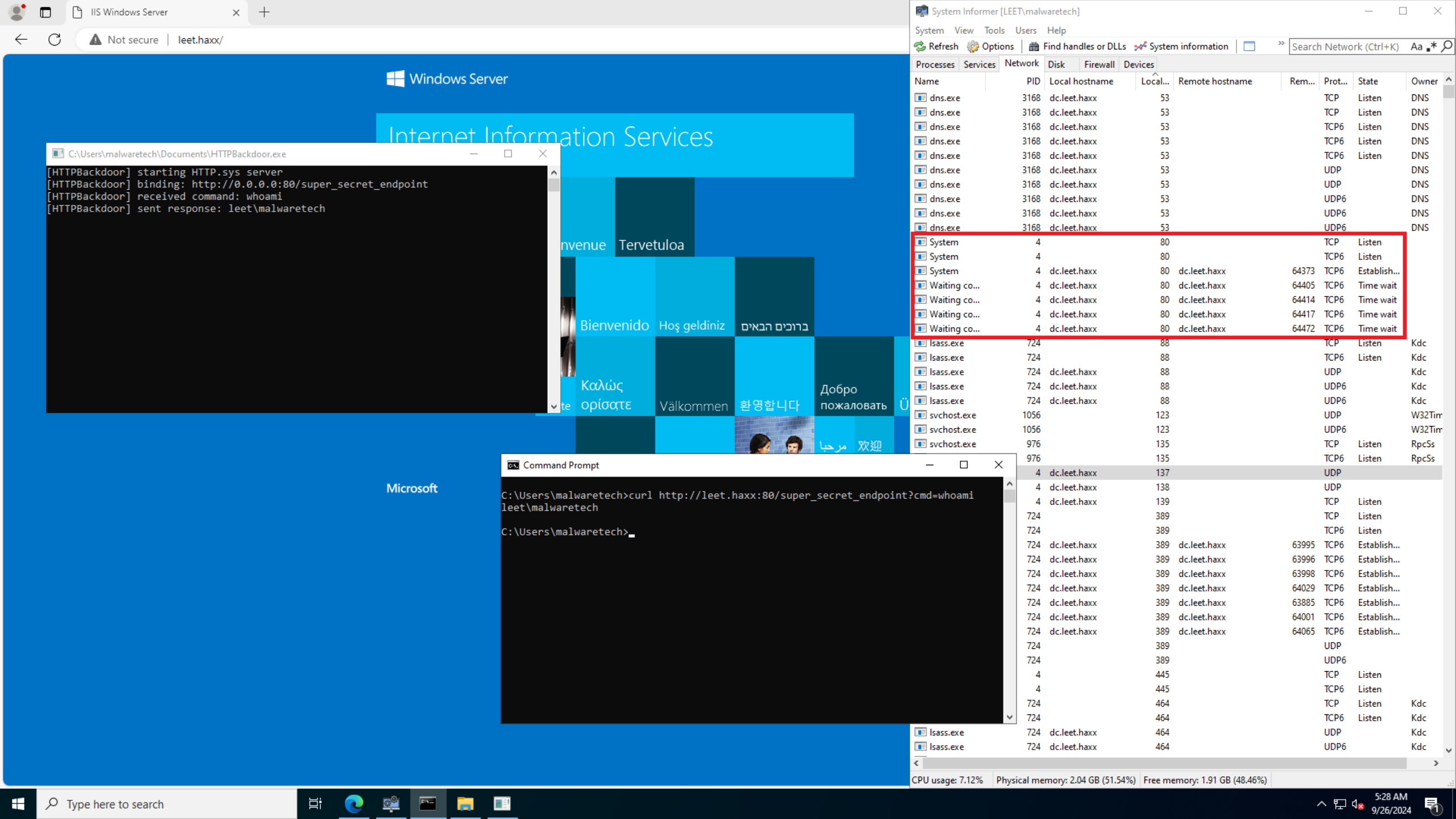
# Stealthy User Mode Backdoors Via The HTTP.sys API

The screenshot displays a Windows Server environment with the following components:

- Internet Information Services (IIS) Windows Server:** The main application window showing the IIS configuration.
- HTTP.sys Service:** A service running in the background, listening on port 80. The command prompt shows the backdoor receiving a 'whoami' command and returning 'leet\malwaretech'.
- System Informer [LEET\malwaretech]:** A tool showing the system's network connections. A red box highlights the listening state of the backdoor, and a list of established connections is shown below.

Name	PID	Local hostname	Local...	Remote hostname	Rem...	Prot...	State	Owner
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			UDP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			UDP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			UDP6	Listen	DNS
System	4		80			TCP	Listen	
System	4		80			TCP6	Listen	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64373	TCP6	Establish...	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64405	TCP6	Time wait	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64414	TCP6	Time wait	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64417	TCP6	Time wait	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64472	TCP6	Time wait	
lsass.exe	724		88			TCP	Listen	Kdc
lsass.exe	724		88			TCP6	Listen	Kdc
lsass.exe	724	dc.leet.haxx	88			UDP		Kdc
lsass.exe	724	dc.leet.haxx	88			UDP6		Kdc
svchost.exe	1056		123			UDP		W32Tim
svchost.exe	1056		123			UDP6		W32Tim
svchost.exe	976		135			TCP	Listen	RpcSs
svchost.exe	976		135			TCP6	Listen	RpcSs
dc.leet.haxx	4		137			UDP		
dc.leet.haxx	4		138			UDP		
dc.leet.haxx	4		139			TCP	Listen	
dc.leet.haxx	724		389			TCP	Listen	
dc.leet.haxx	724		389			TCP6	Listen	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	63995	TCP6	Establish...	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	63996	TCP6	Establish...	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	63998	TCP6	Establish...	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	64029	TCP6	Establish...	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	63885	TCP6	Establish...	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	64001	TCP6	Establish...	
dc.leet.haxx	724	dc.leet.haxx	389	dc.leet.haxx	64065	TCP6	Establish...	
dc.leet.haxx	724		389			UDP		
dc.leet.haxx	724		389			UDP6		
dc.leet.haxx	4		445			TCP	Listen	
dc.leet.haxx	4		445			TCP6	Listen	
dc.leet.haxx	724		464			TCP	Listen	Kdc
dc.leet.haxx	724		464			TCP6	Listen	Kdc
lsass.exe	724	dc.leet.haxx	464			UDP		Kdc
lsass.exe	724	dc.leet.haxx	464			UDP6		Kdc

System Informer [LEET\malwaretech] CPU usage: 7.12% Physical memory: 2.04 GB (51.54%) Free memory: 1.91 GB (48.46%)



Windows Server

Internet Information Services

C:\Users\malwaretech\Documents\HTTPBackdoor.exe

```
[HTTPBackdoor] starting HTTP.sys server
[HTTPBackdoor] binding: http://0.0.0.0:80/super_secret_endpoint
[HTTPBackdoor] received command: whoami
[HTTPBackdoor] sent response: leet\malwaretech
```

venue Tervetuloa

Bienvenido

Hoş geldiniz

ברוכים הבאים

Καλώς

ορίσαστε

Välkommen

환영합니다

Добро

пожаловать

مرحبا

欢迎

Microsoft

Command Prompt

```
C:\Users\malwaretech>curl http://leet.haxx:80/super_secret_endpoint?cmd=whoami
leet\malwaretech
C:\Users\malwaretech>
```

System Informer [LEET\malwaretech]

System View Tools Users Help

Refresh Options Find handles or DLLs System information

Search Network (Ctrl+K) Aa

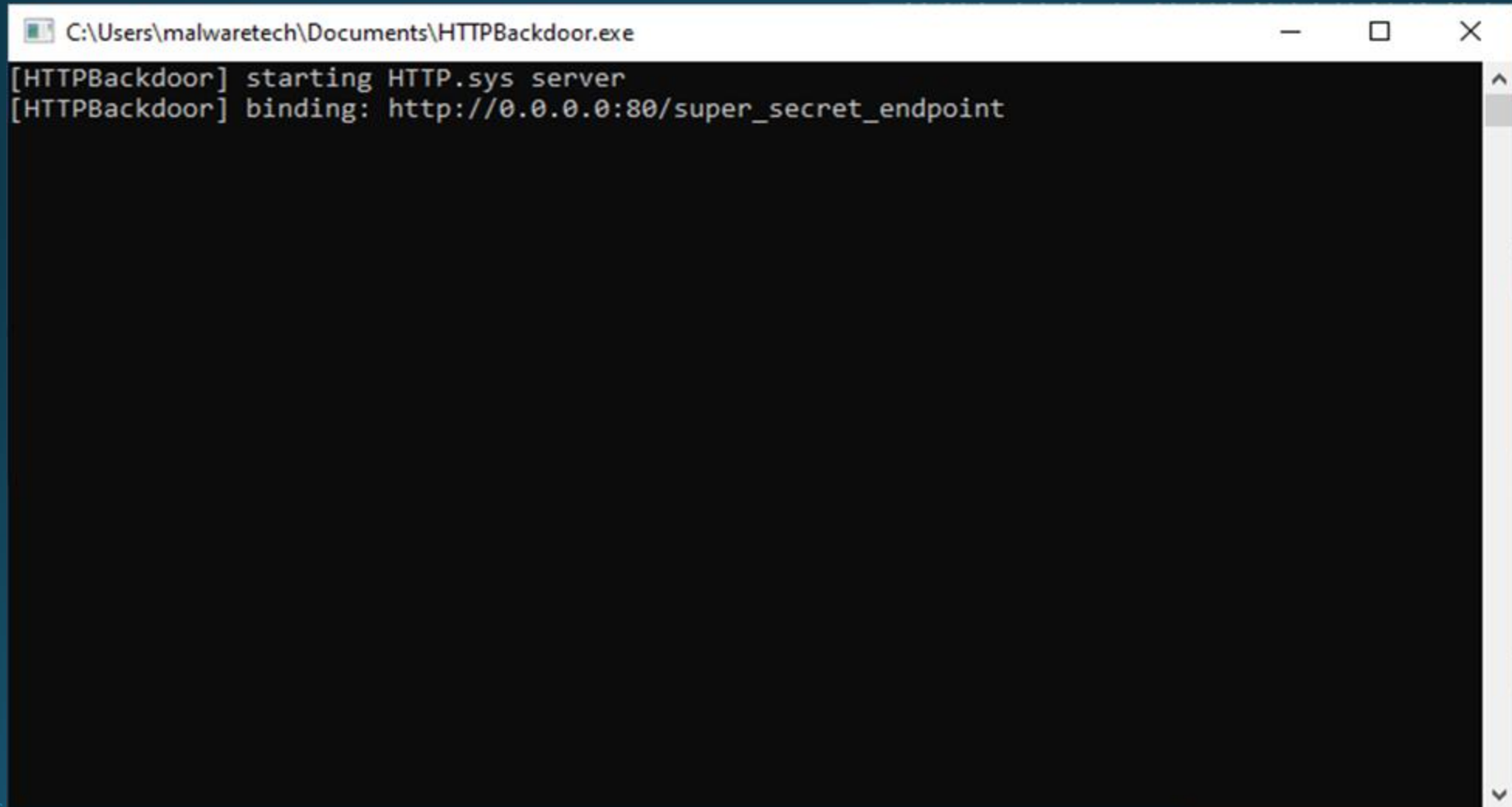
Processes	Services	Network	Disk	Firewall	Devices			
Name	PID	Local hostname	Local...	Remote hostname	Rem...	Prot...	State	Owner
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			UDP		DNS
dns.exe	3168	dc.leet.haxx	53			UDP		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
System	4		80			TCP	Listen	
System	4		80			TCP6	Listen	
System	4	dc.leet.haxx	80	dc.leet.haxx	64373	TCP6	Establish...	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64405	TCP6	Time wait	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64414	TCP6	Time wait	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64417	TCP6	Time wait	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	64472	TCP6	Time wait	
lsass.exe	724		88			TCP	Listen	Kdc
lsass.exe	724		88			TCP6	Listen	Kdc
lsass.exe	724	dc.leet.haxx	88			UDP		Kdc
lsass.exe	724	dc.leet.haxx	88			UDP6		Kdc
lsass.exe	724	dc.leet.haxx	88			UDP6		Kdc
svchost.exe	1056		123			UDP		W32Tir
svchost.exe	1056		123			UDP6		W32Tir
svchost.exe	976		135			TCP	Listen	RpcSs
svchost.exe	976		135			TCP6	Listen	RpcSs
	4	dc.leet.haxx	137			UDP		
	4	dc.leet.haxx	138			UDP		
	4	dc.leet.haxx	139			TCP	Listen	
	724		389			TCP	Listen	
	724		389			TCP6	Listen	
	724	dc.leet.haxx	389	dc.leet.haxx	63995	TCP6	Establish...	
	724	dc.leet.haxx	389	dc.leet.haxx	63996	TCP6	Establish...	
	724	dc.leet.haxx	389	dc.leet.haxx	63998	TCP6	Establish...	
	724	dc.leet.haxx	389	dc.leet.haxx	64029	TCP6	Establish...	
	724	dc.leet.haxx	389	dc.leet.haxx	63885	TCP6	Establish...	
	724	dc.leet.haxx	389	dc.leet.haxx	64001	TCP6	Establish...	
	724	dc.leet.haxx	389	dc.leet.haxx	64065	TCP6	Establish...	
	724		389			UDP		
	724		389			UDP6		
	4		445			TCP	Listen	
	4		445			TCP6	Listen	
	724		464			TCP	Listen	Kdc
	724		464			TCP6	Listen	Kdc
lsass.exe	724	dc.leet.haxx	464			UDP		Kdc
lsass.exe	724	dc.leet.haxx	464			UDP6		Kdc

CPU usage: 7.12% Physical memory: 2.04 GB (51.54%) Free memory: 1.91 GB (48.46%)

5:28 AM

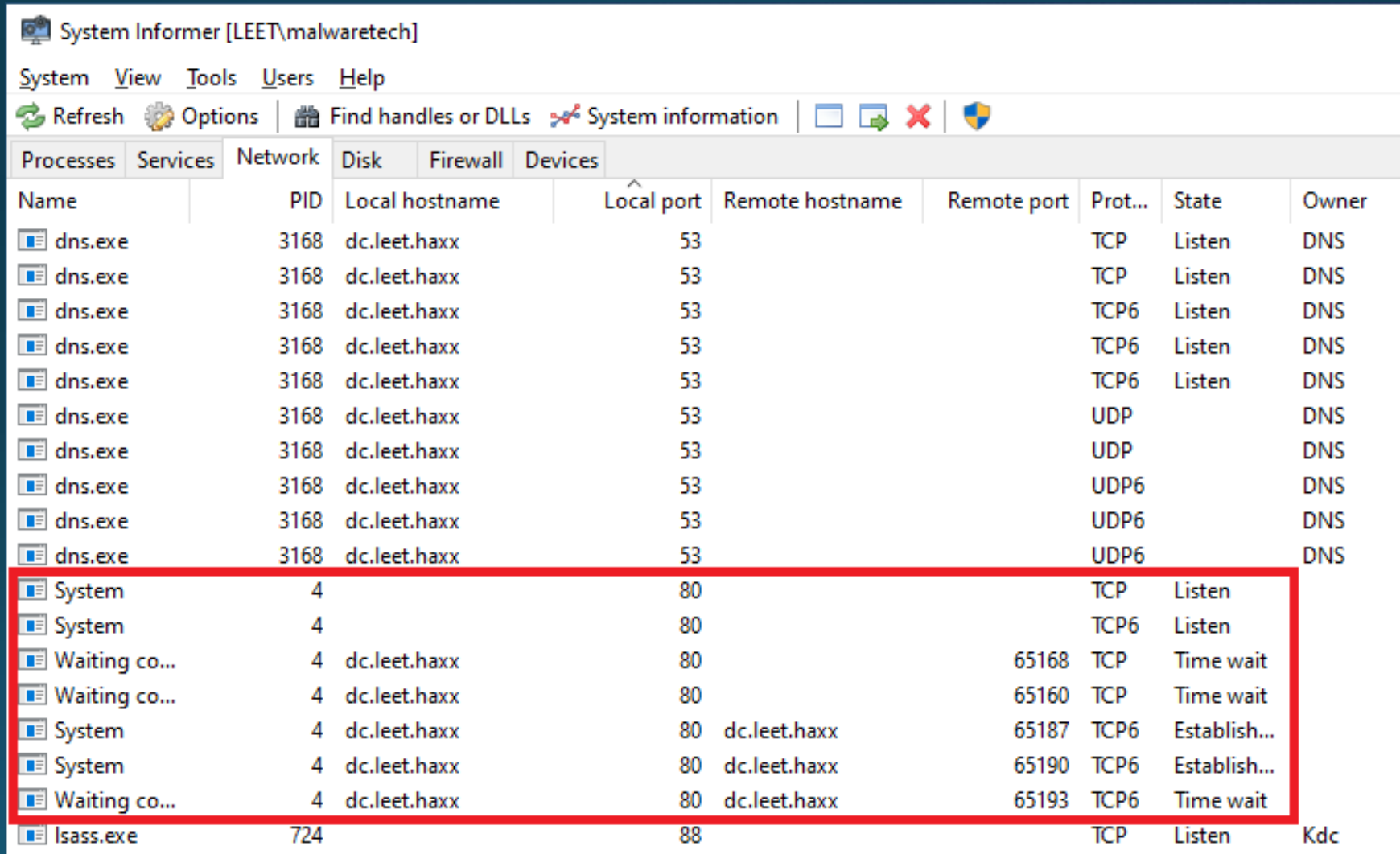
9/26/2024

# http.sys allows us to launch http servers in the kernel from user mode



```
C:\Users\malwaretech\Documents\HTTPBackdoor.exe
[HTTPBackdoor] starting HTTP.sys server
[HTTPBackdoor] binding: http://0.0.0.0:80/super_secret_endpoint
```

# The Windows Kernel binds the port for us and handles the http processing



System Informer [LEET\malwaretech]

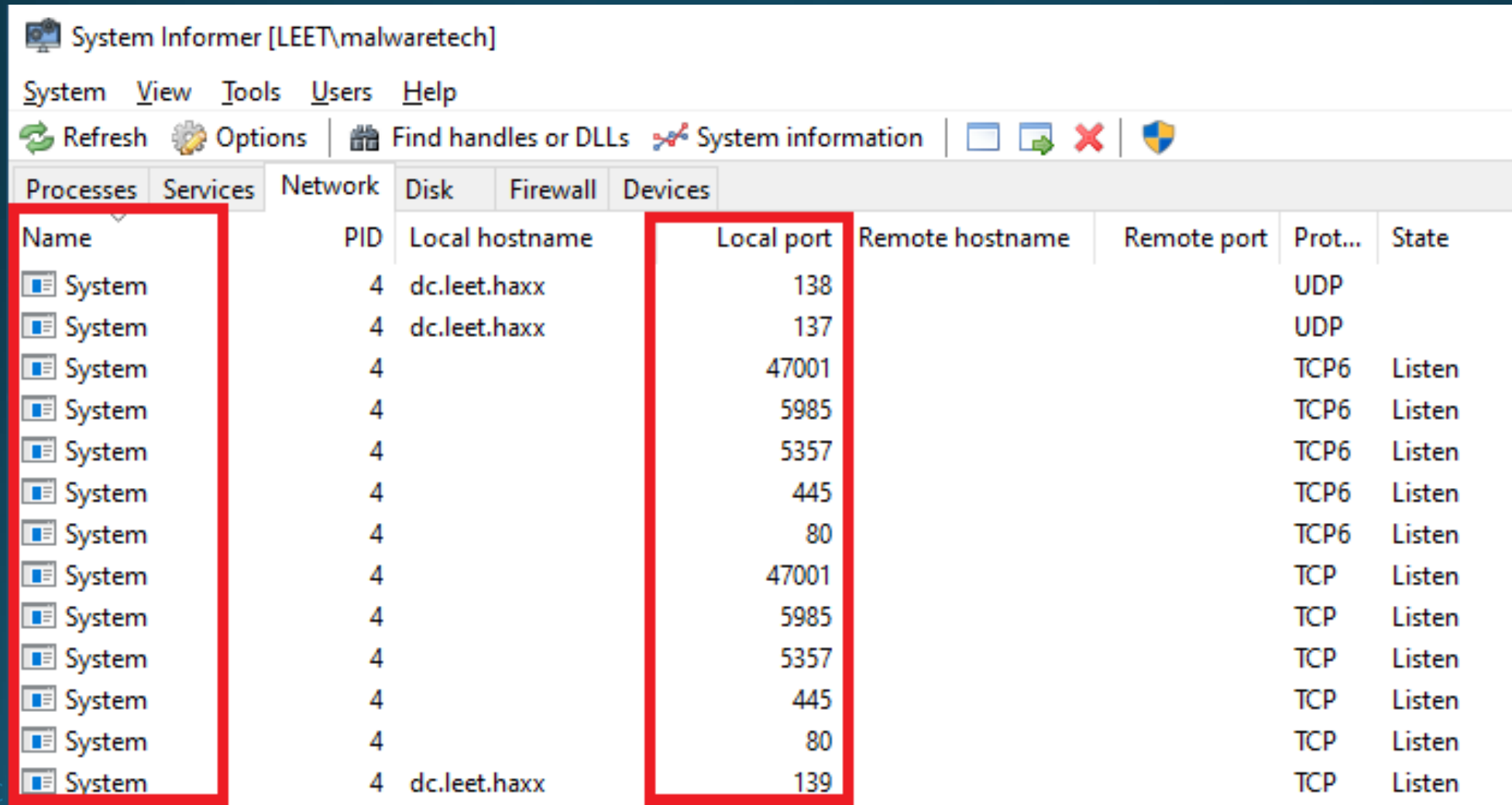
System View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network Disk Firewall Devices

Name	PID	Local hostname	Local port	Remote hostname	Remote port	Prot...	State	Owner
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			UDP		DNS
dns.exe	3168	dc.leet.haxx	53			UDP		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
System	4		80			TCP	Listen	
System	4		80			TCP6	Listen	
Waiting co...	4	dc.leet.haxx	80		65168	TCP	Time wait	
Waiting co...	4	dc.leet.haxx	80		65160	TCP	Time wait	
System	4	dc.leet.haxx	80	dc.leet.haxx	65187	TCP6	Establish...	
System	4	dc.leet.haxx	80	dc.leet.haxx	65190	TCP6	Establish...	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	65193	TCP6	Time wait	
Isass.exe	724		88			TCP	Listen	Kdc

# Since the kernel is responsible for many ports, this isn't unusual



Name	PID	Local hostname	Local port	Remote hostname	Remote port	Prot...	State
System	4	dc.leet.haxx	138			UDP	
System	4	dc.leet.haxx	137			UDP	
System	4		47001			TCP6	Listen
System	4		5985			TCP6	Listen
System	4		5357			TCP6	Listen
System	4		445			TCP6	Listen
System	4		80			TCP6	Listen
System	4		47001			TCP	Listen
System	4		5985			TCP	Listen
System	4		5357			TCP	Listen
System	4		445			TCP	Listen
System	4		80			TCP	Listen
System	4	dc.leet.haxx	139			TCP	Listen

# But It makes it hard to figure out who is really using the port :D

System Informer [LEET\malwaretech]

System View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network Disk Firewall Devices

Name	PID	Local hostname	Local port	Remote hostname	Remote port	Prot...	State	Owner
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			TCP6	Listen	DNS
dns.exe	3168	dc.leet.haxx	53			UDP		DNS
dns.exe	3168	dc.leet.haxx	53			UDP		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
dns.exe	3168	dc.leet.haxx	53			UDP6		DNS
System	4		80			TCP	Listen	
System	4		80			TCP6	Listen	
Waiting co...	4	dc.leet.haxx	80		65168	TCP	Time wait	
Waiting co...	4	dc.leet.haxx	80		65160	TCP	Time wait	
System	4	dc.leet.haxx	80	dc.leet.haxx	65187	TCP6	Establish...	
System	4	dc.leet.haxx	80	dc.leet.haxx	65190	TCP6	Establish...	
Waiting co...	4	dc.leet.haxx	80	dc.leet.haxx	65193	TCP6	Time wait	
Isass.exe	724		88			TCP	Listen	Kdc

# We don't even need to be admin! Some endpoints can be bound by regular users

**Usable by any user, even guest accounts:**

- `http://0.0.0.0:80/Temporary_Listen_Addresses/*`

**Usable by standard users:**

- `http://0.0.0.0:5357/*`  
`http://0.0.0.0:5358/*`

**Usable by any domain user:**

- `http://0.0.0.0:10247/apps/*`

# The default domain firewall profile exposes some of the unprivileged ports

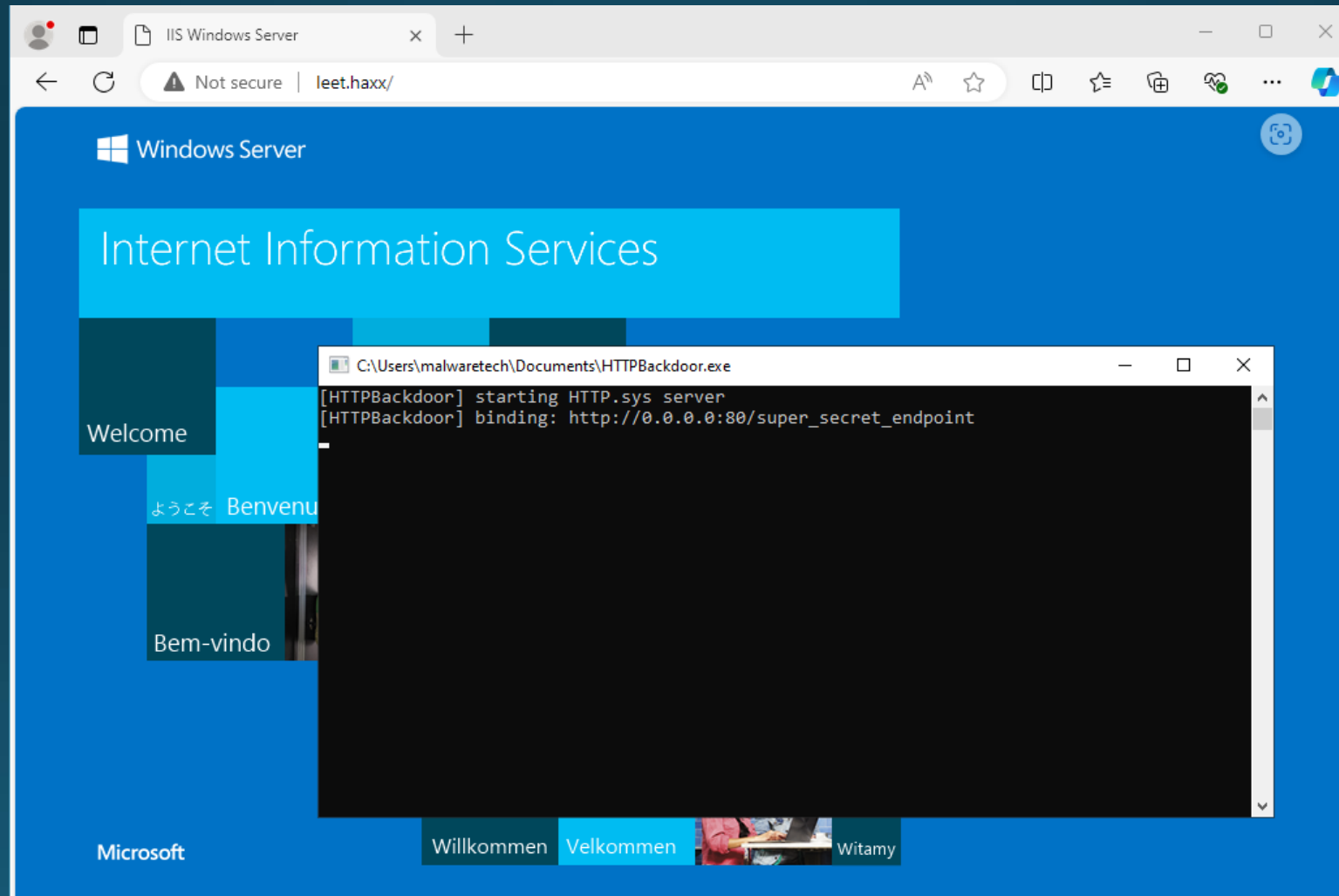
- Port 10247 (open to world)
- Port 5357 (open to world if network discovery is enabled)
- Port 5358 (open to world if network discovery is enabled)



# With Admin privileges, things get even more fun

- We can bind almost any port we want via the System process
- we can also piggyback on certain ports that are already in use by other apps
- If an app is using <http://0.0.0.0:80/app/api>, we could bind a different endpoint on the same port if port sharing is enabled.
- The app won't see any request sent to our endpoint, and we won't see requests sent to theirs!

# IIS uses port sharing, so we can add endpoints to IIS and Outlook Servers



# All Communication with http.sys can be done via IOCTL

- No sockets
- No named pipes
- No DLLs
- Just a nice stealthy backdoor

# This method is used by several Chinese and Iranian APTs to backdoor servers

- <https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/>
- <https://cloud.google.com/blog/topics/threat-intelligence/unc186o-iran-middle-eastern-networks>

# You can investigate endpoints using "netsh http show servicestate"

```
Command Prompt

Registered URLs:
  HTTP://+:5985/WSMAN/
  HTTP://+:47001/WSMAN/

Request queue name: DefaultAppPool
  Version: 2.0
  State: Active
  Request queue 503 verbosity level: Limited
  Max requests: 1000
  Number of active processes attached: 1
  Controller process:
    ID: 3332, image: <?>
  Processes:
    ID: 4304, image: <?>
  Registered URLs:
    HTTP://*:80/

Request queue name: Request queue is unnamed.
  Version: 2.0
  State: Active
  Request queue 503 verbosity level: Basic
  Max requests: 1000
  Number of active processes attached: 1
  Processes:
    ID: 6796, image: C:\Users\malwaretech\Documents\HTTPBackdoor.exe
  Registered URLs:
    HTTP://*:80/SUPER_SECRET_ENDPOINT/
```