

Investigating Windows

Whats the version and year of the windows machine?: **Windows Server 2016**

To learn this question answer lets execute basic powershell command.

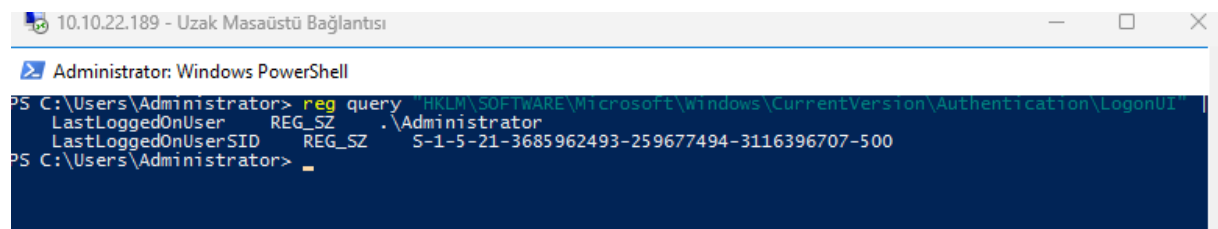
```
PS C:\Users\Administrator> Get-ComputerInfo -Property "Os*"

OsName                : Microsoft Windows Server 2016 Datacenter
OsType                : WINNT
OsOperatingSystemSKU  : DatacenterServerEdition
OsVersion             : 10.0.14393
OsCSDVersion          :
```

Which user logged in last?: **Administrator**

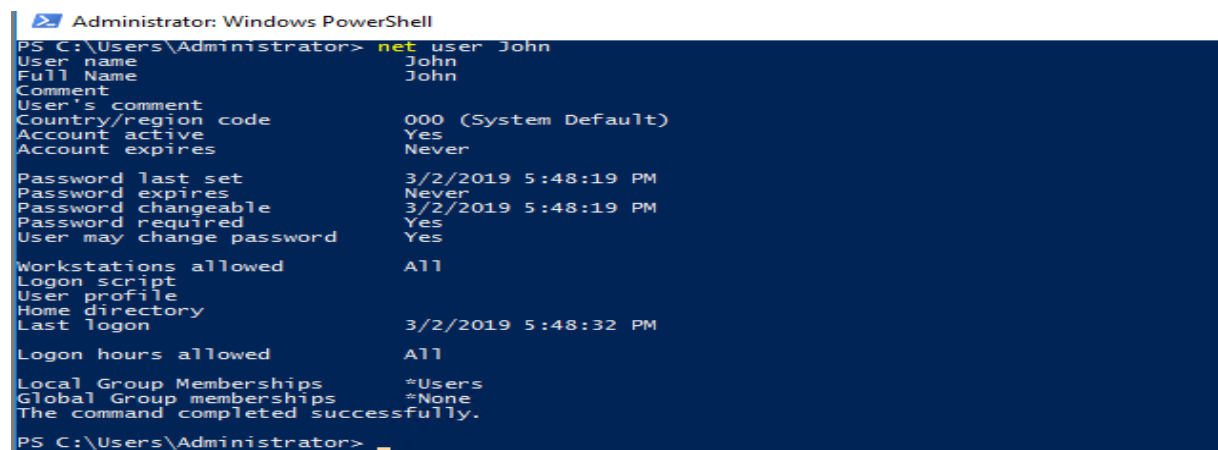
LogonUI key stores configuration settings for the Windows logon and lock screen interface, controlling how the logon screen is displayed and how the user selection/credential interface behaves

```
reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI"
| findstr LastLoggedOnUser
```



```
10.10.22.189 - Uzak Masaüstü Bağlantısı
Administrator: Windows PowerShell
PS C:\Users\Administrator> reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI"
| findstr LastLoggedOnUser
LastLoggedOnUser REG_SZ .\Administrator
LastLoggedOnUserSID REG_SZ S-1-5-21-3685962493-259677494-3116396707-500
PS C:\Users\Administrator>
```

When did John log onto the system last?: **03/02/2019 5:48:32 PM**

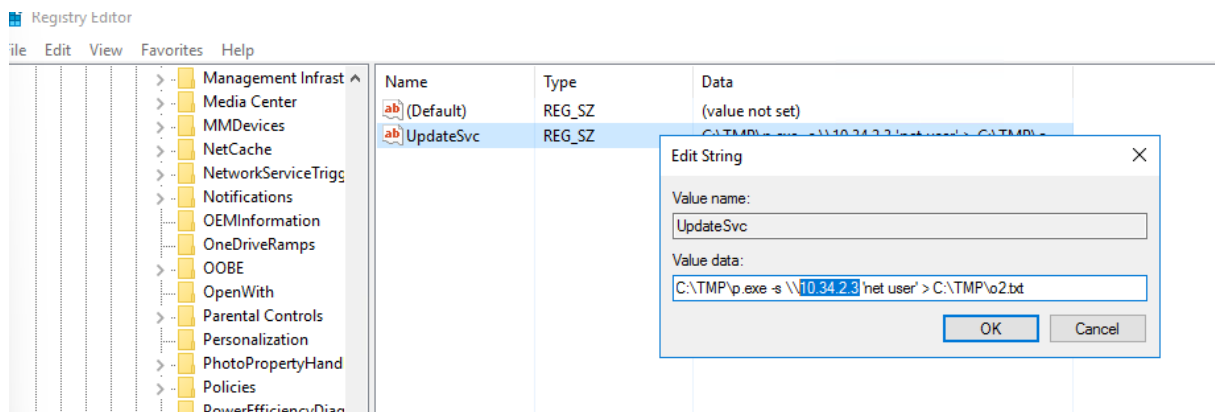


```
Administrator: Windows PowerShell
PS C:\Users\Administrator> net user John
User name                John
Full Name                John
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set         3/2/2019 5:48:19 PM
Password expires          Never
Password changeable       3/2/2019 5:48:19 PM
Password required         Yes
User may change password  Yes
Workstations allowed      All
Logon script
User profile
Home directory
Last logon                3/2/2019 5:48:32 PM
Logon hours allowed       All
Local Group Memberships   *Users
Global Group memberships *None
The command completed successfully.
PS C:\Users\Administrator>
```

What IP does the system connect to when it first starts?: **10.34.2.3**

The question ask when computer start so that we should check below reg key. After checking found suspicious key which is contain C:\TMP directory. Once examine content of the key we have observed IP address for the connection first start.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



What two accounts had administrative privileges (other than the Administrator user)?: **Guest Jenny**

```
More help is available by typing NET HELPMMSG 2221.

PS C:\Users\Administrator> net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
Guest
Jenny
The command completed successfully.

PS C:\Users\Administrator> _
```

Whats the name of the scheduled task that is malicous. : **Clean File System**

We have executed command that is seen below then examined root path and some of suspicious file have been observed. Clean file system is the one of them.

```
The command completed successfully.

PS C:\Users\Administrator> Get-ScheduledTask

TaskPath      TaskName      State
-----
\Microsoft\Windows\TaskScheduler\TaskScheduler\Amazon Ec2 Launch - Instance I... Disabled
\Microsoft\Windows\TaskScheduler\TaskScheduler\check logged in Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\Clean file system Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\falshupdate22 Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\GameOver Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\update windows Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\.NET Framework NGEN v4.0.30319 Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\.NET Framework NGEN v4.0.30319 64 Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\.NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\TaskScheduler\TaskScheduler\.NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\TaskScheduler\TaskScheduler\AD RMS Rights Policy Template ... Disabled
\Microsoft\Windows\TaskScheduler\TaskScheduler\AD RMS Rights Policy Template ... Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\EDP Policy Manager Ready
\Microsoft\Windows\TaskScheduler\TaskScheduler\PolicyConverter Disabled
```

What file was the task trying to run daily? :**nc.ps1**

To find it I have executed this command on the powershell

schtasks /query /tn "Clean file system" /v /fo LIST we know that Clean file system is a malicious file and powershell command executed with filtered. The v parameter provides verbosity, fo indicates readable format and tn is indicates task name.

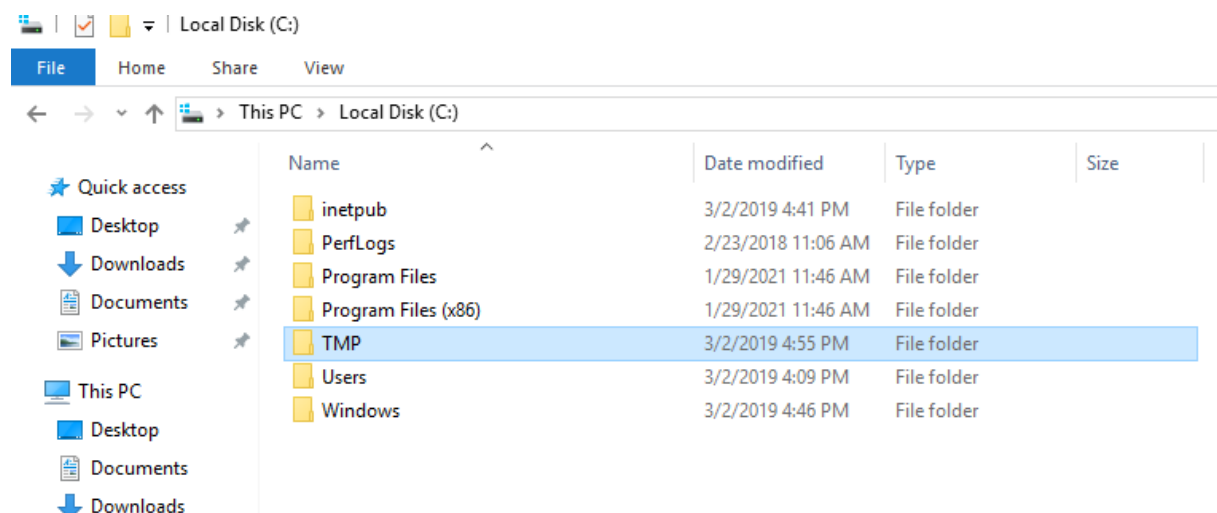
```
PS C:\Users\Administrator> schtasks /query /tn "Clean file system" /v /fo LIST
Folder: \
HostName: EC2AMAZ-I8UH076
TaskName: \Clean file system
Next Run Time: 11/3/2025 4:55:17 PM
Status: Ready
Logon Mode: Interactive only
Last Run Time: 11/2/2025 7:14:06 PM
Last Result: -2147020576
Author: EC2AMAZ-I8UH076\Administrator
Task To Run: C:\TMP\nc.ps1 -l 1348
Start In: N/A
Comment: A task to clean old files of the system
Scheduled Task State: Enabled
Idle Time: Disabled
Power Management: Stop On Battery Mode, No Start On Batteries
Run As User: Administrator
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule: Scheduling data is not available in this format.
Schedule Type: Daily
Start Time: 4:55:17 PM
Start Date: 3/2/2019
End Date: N/A
Days: Every 1 day(s)
Months: N/A
Repeat: Every: Disabled
Repeat: Until: Time: Disabled
Repeat: Until: Duration: Disabled
Repeat: Stop If Still Running: Disabled
PS C:\Users\Administrator>
```

What port did this file listen locally for?:**1348**

Detailed above PNG

At what date did the compromise take place?:**03/02/2019**

TMP directory is should not be stored C:\ also we know that stores a malicious file which is named ns.ps1. So that we can get reference this file modified time as a compromise take place date.



When did Jenny last logon?: **Never**

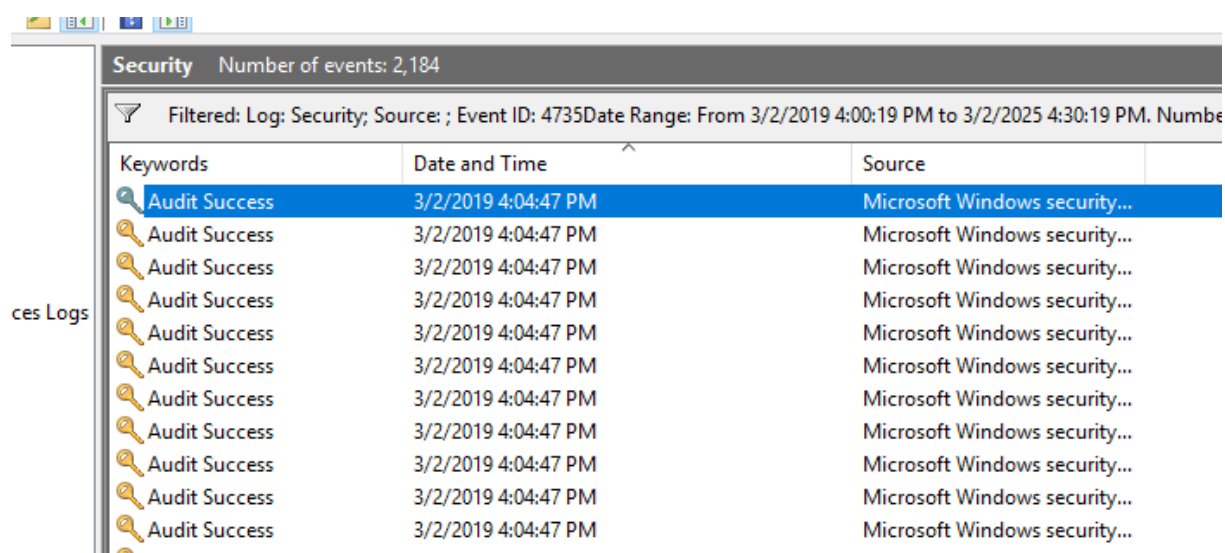
```
PS C:\Users\Administrator> net user Jenny
User name                Jenny
Full Name                Jenny
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        3/2/2019 4:52:25 PM
Password expires         Never
Password changeable      3/2/2019 4:52:25 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never
Logon hours allowed      All
```

During the compromise, at what time did Windows first assign special privileges to a new logon?: 3/2/2019

To see this answer examined after the compromised date special privilege login and I have looked at the first Security Group Management change after the this time.



What tool was used to get Windows passwords?:**Mimikatz**

Even you were in navigate on normal interface on the windows you might be observed cmd.exe open and close frequently. If you examined what process executed you must observe mim.exe.

```

##### mimikatz 2.0 alpha (x86) release "Kiwi en C" (Feb 16 2015 22:17:52)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 15 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 195072 (00000000:0002fa00)
Session : Interactive from 1
User Name : Ion
Domain : Ion-PC
SID : S-1-5-21-2367887663-2567669145-1589166190-1000

msv :
[00000003] Primary
* Username : Ion
* Domain : Ion-PC
* NTLM : a4a9436b46f7e948b2417435b63d6cac
* SHA1 : 6c69a6cc3e5313a83fde6d27256b17e5020ffcb5
[00010000] CredentialKeys
* NTLM : a4a9436b46f7e948b2417435b63d6cac
* SHA1 : 6c69a6cc3e5313a83fde6d27256b17e5020ffcb5

```

What was the attackers external control and command servers IP?:**76.32.97.132**

When you open the below path and hosts file you will see the recorded DNS names. So that some of the DNS names already suspicious. When ping to google on another pc detected this is not a google.com it is redirecting fake or abnormal site.

```

#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com      # source server
#       38.25.63.10     x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
10.2.2.2      update.microsoft.com
127.0.0.1     www.virustotal.com
127.0.0.1     www.www.com
127.0.0.1     dci.sophosupd.com
10.2.2.2      update.microsoft.com
127.0.0.1     www.virustotal.com
127.0.0.1     www.www.com
127.0.0.1     dci.sophosupd.com
10.2.2.2      update.microsoft.com
127.0.0.1     www.virustotal.com
127.0.0.1     www.www.com
127.0.0.1     dci.sophosupd.com
76.32.97.132 google.com
76.32.97.132 www.google.com

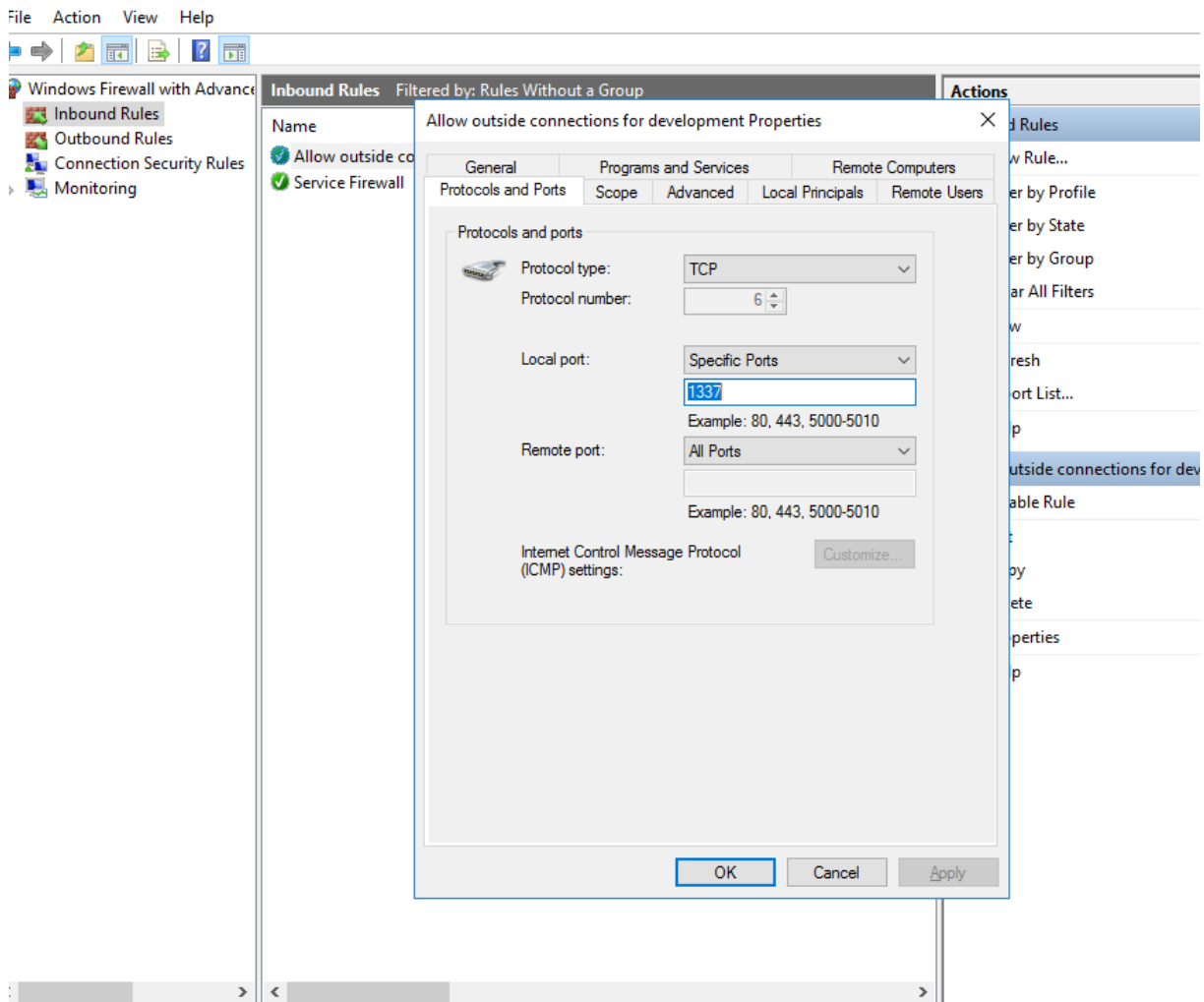
```

What was the extension name of the shell uploaded via the servers website?:**.jsp**

Asking website so that we know the other suspicious directory is a inetpub and when we go through itself and after the examination wwwroot directory observed and this is C2 web site file store.

This PC > Local Disk (C:) > inetpub > wwwroot				
	Name	Date modified	Type	Size
ick access	b	3/2/2019 4:37 PM	JSP File	74 KB
esktop	shell	3/2/2019 4:37 PM	GIF File	13 KB
ownloads	tests	3/2/2019 4:37 PM	JSP File	1 KB
ocuments				
ictures				

What was the last port the attacker opened?:1337



Check for DNS poisoning, what site was targeted?:**google.com**

```
127.0.0.1 dci.sophosupd.com
76.32.97.132 google.com
76.32.97.132 www.google.com
```