Technical Analysis of Copybara

zscaler.com/blogs/security-research/technical-analysis-copybara

Ruchna Nigam

Introduction

Zscaler ThreatLabz recently analyzed a new variant of Copybara, which is an Android malware family that emerged in November 2021. The malware is primarily spread through voice phishing (vishing) attacks, where victims receive instructions over the phone to install the Android malware.

This new variant of Copybara has been active since November 2023, and utilizes the MQTT protocol to establish communication with its command-and-control (C2) server. The malware abuses the Accessibility Service feature that is native to Android devices to exert granular control over the infected device. In the background, the malware also proceeds to download phishing pages that imitate popular cryptocurrency exchanges and financial institutions with the use of their logos and application names. These pages are designed to deceive victims into entering their credentials, which can then be stolen by the malware.

This blog offers valuable insights into Copybara malware and presents a comprehensive technical analysis of the 59 supported commands.. Although the exact method of luring victims into downloading this specific variant is unknown, the URLs hosting these malicious applications have been identified and shared as indicators of compromise (IOCs).

Key Takeaways

- Copybara is an Android malware family that dates back to 2021 and was last updated November 2023.

- The malware is a trojan with a significant number of capabilities including keylogging, audio & video recording, SMS hijacking, screen capturing, credential stealing, and remotely controlling an infected device.
- Copybara is frequently observed impersonating popular applications for financial institutions in Italy and Spain and downloading phishing pages imitating cryptocurrency exchanges and global financial institutions.
- A notable addition in the most recent variant of Copybara is the utilization of the MQTT protocol for communication with the C2 server.

Overview

The latest Copybara variant utilizes the MQTT protocol for communications with the C2 server. MQTT is a lightweight messaging protocol specifically designed for efficient communication between devices that may have limited resources or operate in environments with restricted network bandwidth, such as those found in an Internet of Things (IoT) context.

Similar to its predecessor, this variant of Copybara has been developed using B4A, which is a legitimate framework commonly used for creating Android applications. Most of the Copybara samples analyzed impersonate well known financial institutions in Italy and Spain. The logos for some prominent financial institutions that are impersonated by Copybara are shown in the figure below.

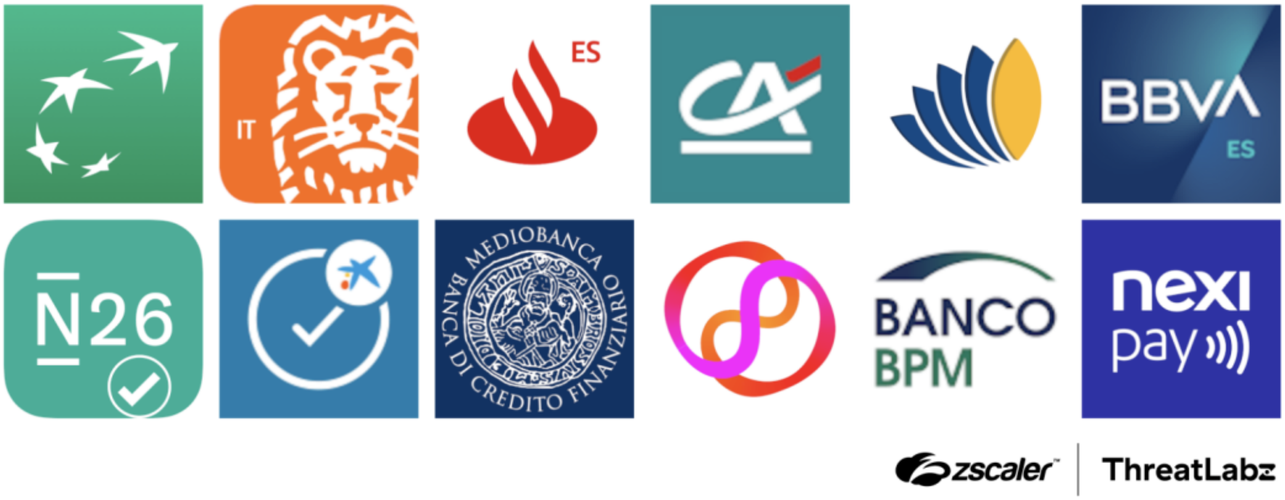
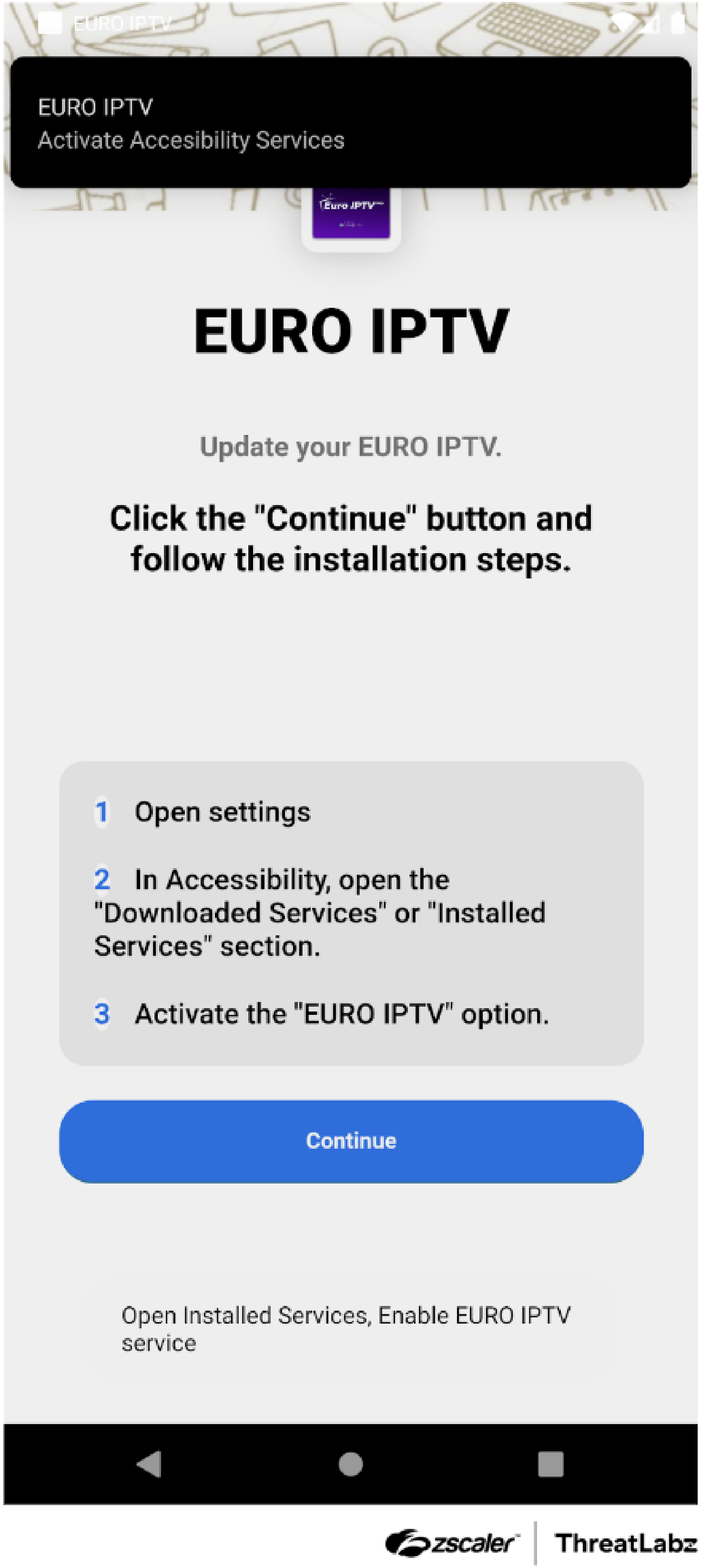


Figure 1: Logos of financial institutions impersonated by Copybara.

In addition, we came across some versions of Copybara impersonating Google Chrome and an IPTV application, as shown in the figure below.



EURO IPTV

Activate Accesibility Services

EURO IPTV

Update your EURO IPTV.

Click the "Continue" button and follow the installation steps.

1 Open settings

2 In Accessibility, open the "Downloaded Services" or "Installed Services" section.

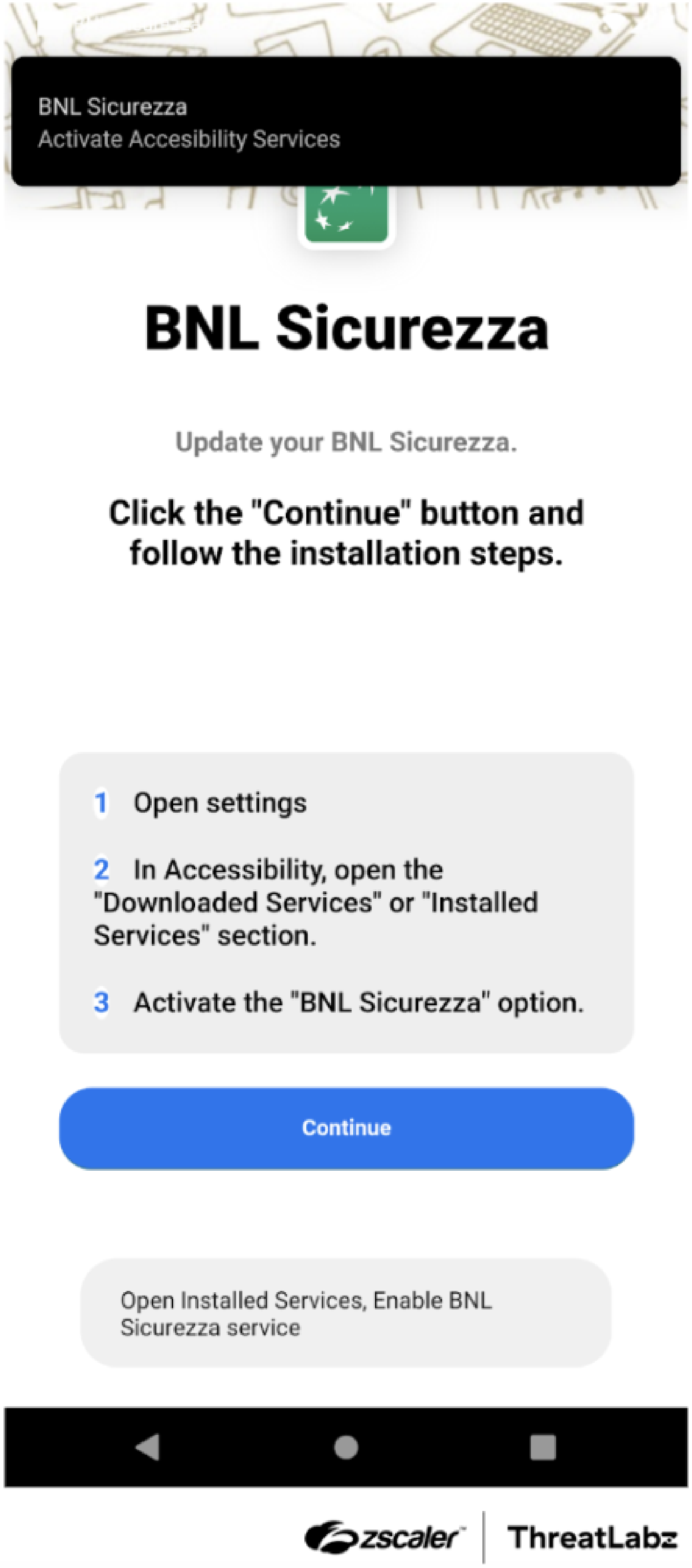
3 Activate the "EURO IPTV" option.

Open Installed Services, Enable EURO IPTV service

Figure 2: Example Copybara disguised as an IPTV application.

Technical Analysis

Upon launching the application, the user is shown an attacker-defined message screen asking the user to enable the Accessibility Service permission for the application, as shown in the figure below. The Accessibility Service is a legitimate feature on Android phones to assist users with disabilities, however due to the inherent nature of the service, the feature may provide a threat actor with highly granular control over a victim's phone if enabled. If Copybara is installed and not granted the accessibility permission, the malware repeatedly shows notifications and toast messages (as shown in the figure below) to coerce the victim into enabling the service.



BNL Sicurezza
Activate Accesibility Services

BNL Sicurezza

Update your BNL Sicurezza.

Click the "Continue" button and follow the installation steps.

1 Open settings

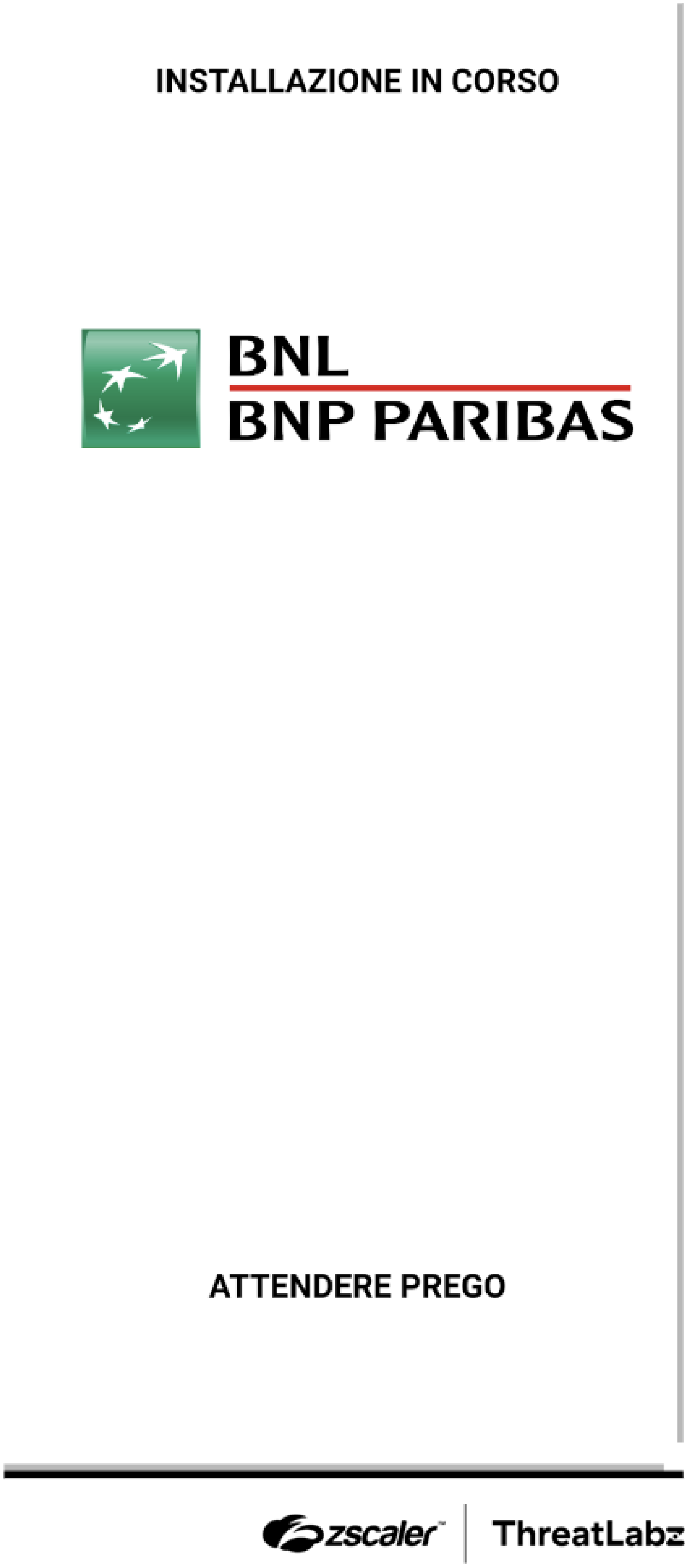
2 In Accessibility, open the "Downloaded Services" or "Installed Services" section.

3 Activate the "BNL Sicurezza" option.

Open Installed Services, Enable BNL Sicurezza service

Figure 3 : Example Copybara launch screen without the accessibility permission enabled.

If the service is enabled, the user is shown another attacker-defined screen, as shown in the figure below.



INSTALLAZIONE IN CORSO

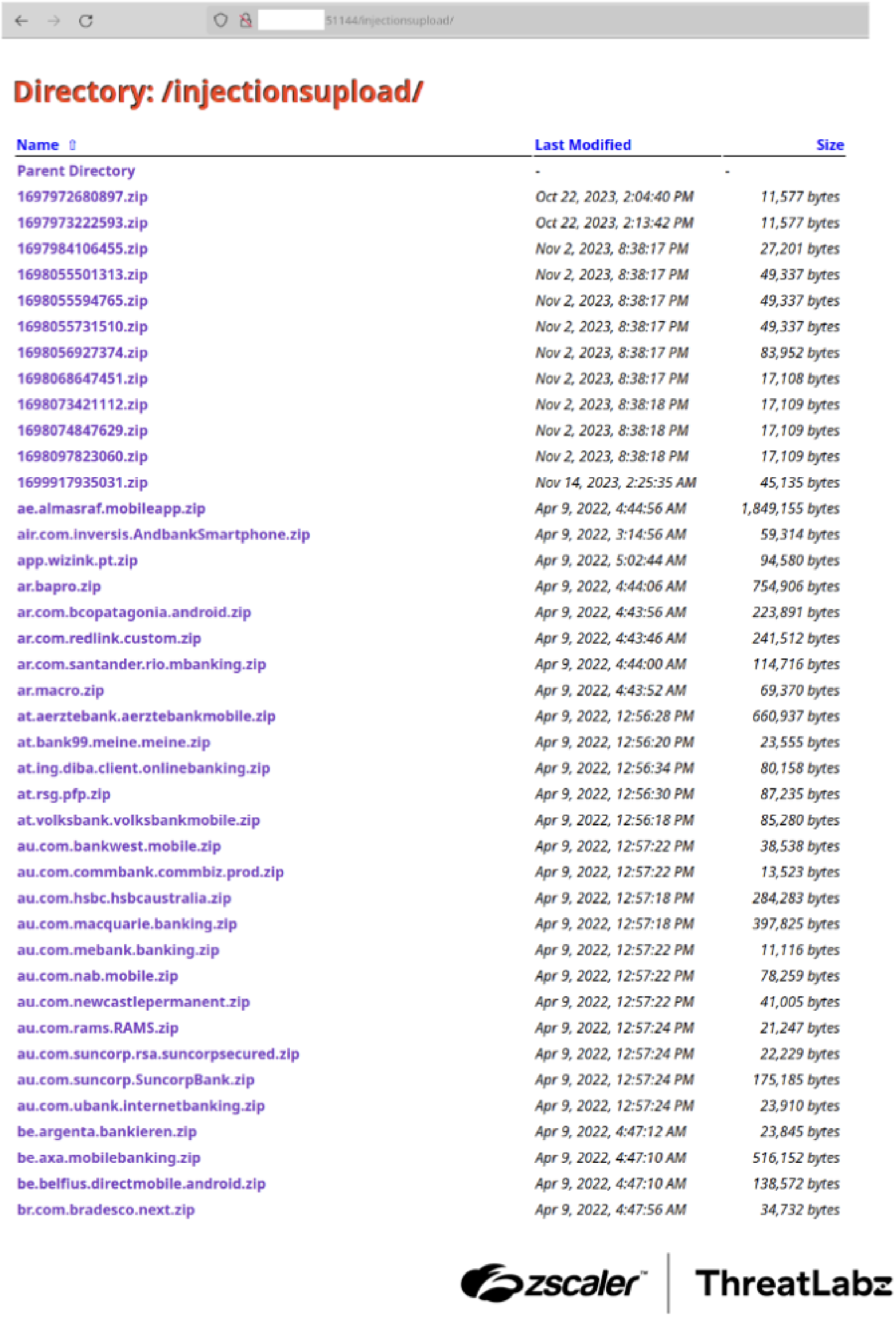
ATTENDERE PREGO

Figure 4: Example screenshot of Copybara after the Accessibility Service feature is enabled.

Once the Accessibility Service feature is enabled, the application prevents the user from accessing some options in the Settings menu, ensuring they are unable to uninstall Copybara. In the background, the malware's behavior is determined by its configuration. Copybara is designed to download a list of phishing pages from the

C2 server. The Copybara C2 responds with a ZIP file containing counterfeit login pages that mimic popular cryptocurrency exchanges and financial institutions. During our analysis, we discovered the existence of two operational C2 servers that were actively serving the phishing pages.

The figure below shows an open directory of a live C2 server hosting Copybara phishing pages.



Directory: /injectionsupload/

Name ⇧	Last Modified	Size
Parent Directory	-	-
1697972680897.zip	Oct 22, 2023, 2:04:40 PM	11,577 bytes
1697973222593.zip	Oct 22, 2023, 2:13:42 PM	11,577 bytes
1697984106455.zip	Nov 2, 2023, 8:38:17 PM	27,201 bytes
1698055501313.zip	Nov 2, 2023, 8:38:17 PM	49,337 bytes
1698055594765.zip	Nov 2, 2023, 8:38:17 PM	49,337 bytes
1698055731510.zip	Nov 2, 2023, 8:38:17 PM	49,337 bytes
1698056927374.zip	Nov 2, 2023, 8:38:17 PM	83,952 bytes
1698068647451.zip	Nov 2, 2023, 8:38:17 PM	17,108 bytes
1698073421112.zip	Nov 2, 2023, 8:38:18 PM	17,109 bytes
1698074847629.zip	Nov 2, 2023, 8:38:18 PM	17,109 bytes
1698097823060.zip	Nov 2, 2023, 8:38:18 PM	17,109 bytes
1699917935031.zip	Nov 14, 2023, 2:25:35 AM	45,135 bytes
ae.almasraf.mobileapp.zip	Apr 9, 2022, 4:44:56 AM	1,849,155 bytes
air.com.inversis.AndbankSmartphone.zip	Apr 9, 2022, 3:14:56 AM	59,314 bytes
app.wizink.pt.zip	Apr 9, 2022, 5:02:44 AM	94,580 bytes
ar.bapro.zip	Apr 9, 2022, 4:44:06 AM	754,906 bytes
ar.com.bcopatagonia.android.zip	Apr 9, 2022, 4:43:56 AM	223,891 bytes
ar.com.redlink.custom.zip	Apr 9, 2022, 4:43:46 AM	241,512 bytes
ar.com.santander.rio.mbanking.zip	Apr 9, 2022, 4:44:00 AM	114,716 bytes
ar.macro.zip	Apr 9, 2022, 4:43:52 AM	69,370 bytes
at.aerztebank.aerztebankmobile.zip	Apr 9, 2022, 12:56:28 PM	660,937 bytes
at.bank99.meine.meine.zip	Apr 9, 2022, 12:56:20 PM	23,555 bytes
at.ing.diba.client.onlinebanking.zip	Apr 9, 2022, 12:56:34 PM	80,158 bytes
at.rsg.pfp.zip	Apr 9, 2022, 12:56:30 PM	87,235 bytes
at.volksbank.volksbankmobile.zip	Apr 9, 2022, 12:56:18 PM	85,280 bytes
au.com.bankwest.mobile.zip	Apr 9, 2022, 12:57:22 PM	38,538 bytes
au.com.commbank.commbiz.prod.zip	Apr 9, 2022, 12:57:22 PM	13,523 bytes
au.com.hsbc.hsbcaustralia.zip	Apr 9, 2022, 12:57:18 PM	284,283 bytes
au.com.macquarie.banking.zip	Apr 9, 2022, 12:57:18 PM	397,825 bytes
au.com.mebank.banking.zip	Apr 9, 2022, 12:57:22 PM	11,116 bytes
au.com.nab.mobile.zip	Apr 9, 2022, 12:57:22 PM	78,259 bytes
au.com.newcastlepermanent.zip	Apr 9, 2022, 12:57:22 PM	41,005 bytes
au.com.rams.RAMS.zip	Apr 9, 2022, 12:57:24 PM	21,247 bytes
au.com.suncorp.rsa.suncorpsecured.zip	Apr 9, 2022, 12:57:24 PM	22,229 bytes
au.com.suncorp.SuncorpBank.zip	Apr 9, 2022, 12:57:24 PM	175,185 bytes
au.com.ubank.internetbanking.zip	Apr 9, 2022, 12:57:24 PM	23,910 bytes
be.argenta.bankieren.zip	Apr 9, 2022, 4:47:12 AM	23,845 bytes
be.axa.mobilebanking.zip	Apr 9, 2022, 4:47:10 AM	516,152 bytes
be.belfius.directmobile.android.zip	Apr 9, 2022, 4:47:10 AM	138,572 bytes
br.com.bradesco.next.zip	Apr 9, 2022, 4:47:56 AM	34,732 bytes

Figure 5: Open directory of a live Copybara C2 server hosting phishing pages.

These phishing pages are designed to deceive unsuspecting users into entering their sensitive information. As depicted in the figure below, an example of one such phishing page imitates a login page for a prominent cryptocurrency exchange.

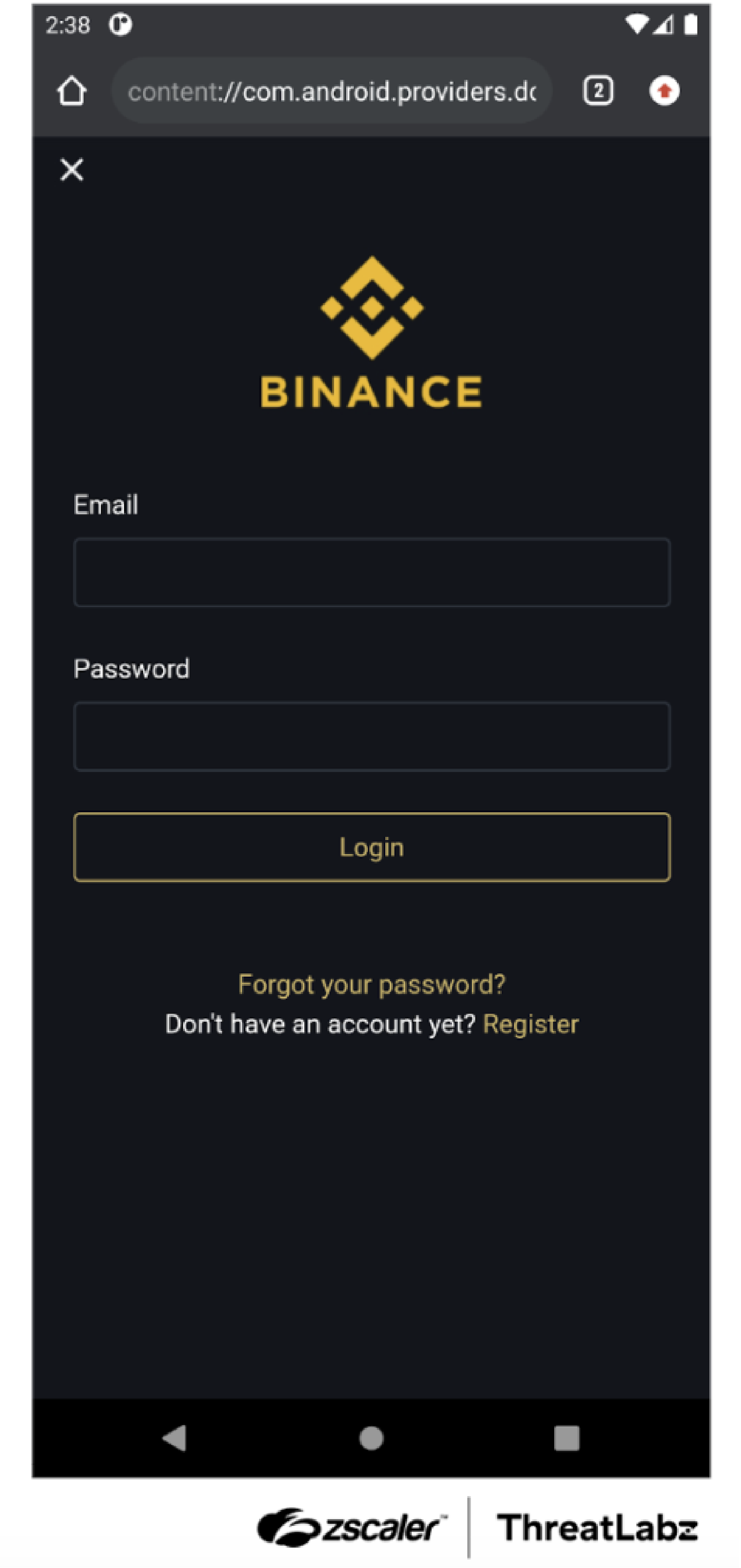

2:38
content://com.android.providers.dc
2
BINANCE
Email
Password
Login
Forgot your password?
Don't have an account yet? Register
zscaler
ThreatLabz

Figure 6: An example Copybara phishing page designed to look like a popular cryptocurrency exchange.

Finally, the application initiates a connection to an MQTT server on port 52997. Copybara subscribes to a specific queue named `commands_FromPC` on this server. This connection enables the application to listen for and receive various commands sent by the C2 server.

The specific commands and their descriptions are provided in the table below.

Command	Functionality
open_app_setngs	Opens Settings for the application (otherwise blocked for the user via the Settings menu).
send_admn_lckdvcs_on	Checks if the device admin feature is enabled. If it is not enabled, the user is prompted to enter a new lock screen password. Subsequently, the malware proceeds to lock the device screen.
send_inj_lst	The malware receives a list of package and filenames associated with injects from the C2 server. If a file with a matching name already exists, the malware first deletes the existing file. Subsequently, it proceeds to download a new file from the C2 server. The downloaded file is then written to disk.
send_custom_opencam	Initializes an MQTT connection to the C2 server and then starts the device's rear camera.
send_custom_opencam2	Initializes an MQTT connection to the C2 server and then starts the device's front camera.
send_custom_opencam_close	Ends camera activity.
send_custom_fullbright	Maximizes screen brightness.
send_custom_lowbright	Minimizes screen brightness.
send_custom_openmics	Transmits audio from the microphone to the C2 server.
send_custom_openmics_close	Stops transmitting microphone audio to the C2 server.
send_custom_delallnoties	Deletes all notifications from the victim's device.
send_custom_donotdelallnoties	Stops deleting notifications.
send_custom_pagebuilder	Creates a custom view using settings from the PB_Data object received from the C2 server. The object contains parameters specifying field types and text specifications to construct a custom webview on-the-fly.
clickbyid	Clicks on the screen at the location specified by gesclick, which is received from the C2 server.
del_my_dv_fm_admnpnl	Closes the connection to the MQTT server and stops the background service.

`Send_Open_Recents`	Shows an overview of recent applications.
`downextraapp`	Downloads an application from an `appurl` parameter provided by the C2 server, saves it under the filename `emptyapp.apk`, and installs it.
`openanyurl`	Opens a URL provided by the C2 server.
`Refrech_hvn_by_Noti`	Dismisses open notifications.
`GlobalParamsActions`	Performs an action specified by the C2 server. The IDs specified by the C2 server correspond to the global actions provided by the Accessibility Service.
`Enable_Noti`	Based on the value of the `Action` flag received from the server, the malware dismisses notifications.
`isAutoSystDalogClker`	Based on the value of the `Action` flag received from the server, the malware takes measures to restrict access to certain options in the Settings menu. This is done to prevent the uninstallation of the malware by the user.
`Request_TurnoffDeviceScreen_FromAndroid`	Turns off the screen capture feature on the victim's device.
`Send_DeviceScreenShot_Permission`	Streams the screen activity of the infected device to the MQTT server. The stream is published to the MQTT server in a queue named `med`.
`Send_Custom_LockScreen`	Downloads an image from the C2 server. The specific image name, referred to as `ImgName`, is provided by the server. Once downloaded, the image is saved as a file named `locscreen.jpg`. However, this functionality is not currently being utilized in the code.
`Send_LockScreen_Overlay`	Minimizes screen brightness and sets a black background.
`Send_LockScreen_Overlay_URL`	Displays a webview that opens a specific URL provided by the server through the `urllink` parameter.
`Send_LockScreen_Overlay_CO`	Displays a webview containing HTML content that is determined by objects received from the server, such as `toptitle`, `bottomtitle`, and `imgurl`. The `imgurl` object can either be a local file path or the name of a URI located on the server. In the case of a URI, it is fetched from the C2 server.
`Send_UnLockScreen_Overlay`	Removes an overlay from the screen.

`Request_HVNC_TableTexts_FromAndroid`	Sets a flag value based on the `isShowingOnlyTable` parameter received from the server. However, this functionality is not currently utilized in the code.
`Send_DeviceApps`	Retrieves a list of installed packages on the infected device and sends this information to the MQTT server by publishing it to a queue called `divap_topc`.
`Send_KeyLo_Views`	Enables or disables the keylogger functionality based on the value of the `IsKeyLo` parameter received from the C2 server.
`Send_Click_FromPCToAndroidDevice`	Carries out a gesture on the screen based on the values `clickstartx`, `clickstarty`, `clickx`, and `clicky` which are provided by the C2 server.
`Send_Text_FromPCToAndroidDevice`	Sets the text value, as specified by the `textvalue` parameter, to the currently focused node on the screen (equivalent to injecting keystrokes).
`Send_Important_Views_Only`	Sets a flag based on the value of the `isImportantViewsOnly` parameter received from the C2 server. However, this flag is not currently utilized in the code.
`FormatthisDevice`	Clears browser history and wipes data on the device.
`Send_CallPhoneNumber`	Initiates a phone call to a specific number provided by the C2 server through the `phonenumber` parameter.
`Send_Change_H_Quality`	Adjusts the image quality of screenshots sent to the C2 server based on the value provided by the `intqulaity` parameter received from the C2 server.
`Get_Device_CallLogs`	Publishes contact information from the device to the MQTT server at a queue named `Device_Calls_Logs_Save`.
`Send_GlobalAction_FromPCToAdroid`	Executes an Accessibility Service action on the phone, depending on the value of the `Action` parameter received from the C2 server.
`Send_ChangeVNCFPS`	Adjusts the frames per second (fps) value based on the `fpsdata` parameter received from the C2 server. This adjustment is made when sending images to the server.
`Hide_AppData_Info`	Hides or displays the application icon in the phone menu based on the value of the `isshouldshow` parameter received from the C2 server.
`Send_Wakeup_Device`	Disables the lock screen.

`Send_Request_Permissions`	Requests a specific permission based on the value of the `permission` parameter received from the C2 server.
`Send_Open_CertainApp`	Initiates the launch of a specific application as indicated by the `apppackage` parameter received from the C2 server.
`Send_Uninstall_CertainApp`	Deletes a specific application, as indicated by the `apppackage` parameter received from the C2 server.
`Send_blocknoti_CertainApp`	Enables the blocking of notifications for a specific application as indicated by the `apppackage` parameter received from the C2 server.
`Send_Block_Certain_App`	Blocks the user from opening a specific application as indicated by the `apppackage` parameter received from the C2 server.
`Send_Swipe_Action_ACS`	Performs a swipe action using the values `firstX`, `firstY`, `secondX`, `secondY`, and `intSpeed` provided by the C2 server.
`Send_Swipe_wheel_Action_ACS`	Performs a swipe action using the values for firstX, firstY, secondX, secondY, and intSpeed provided by the C2 server.
`Send_fromtblclick_ACS`	Performs a swipe action using the values for `firstX`, `firstY`, `secondX`, `secondY`, and `intSpeed` provided by the C2 server.
`Send_Pattren_Action_ACS`	Enters a pattern using the values `firstX`, `firstY`, `secondX, secondY`, and `intSpeed` provided by the C2 server.
`Send_PZ_Action_ACS`	Performs a gesture using the values for `movx1`, `movy1`, `line1X`, `Line1Y`, `movx2`, `movy2`, `line2X`, `Line2Y`, and `intSpeed` provided by the C2 server.
`Send_Create_Notification`	Creates a notification using the data received from the C2 server through the parameters `title`, `description`, `filename`, and `pkgname`. The `filename` object is utilized to download an icon image from the C2 server.
`Send_Show_Pattren_Buttons`	Sets a flag based on the value of the `IsPattren` parameter received from the C2 server. However, this flag is not currently used in the code.
`SendSMS_To_Admin`	Publishes SMS messages collected from the infected device to the MQTT server at a queue named `Send_SMS_To_Admin_From_Android`.

`del_SMS_FromAdmin`	Deletes a specific SMS from the phone as indicated by the `smsid` parameter received from the server.
`Send_SMSMessage_ToNumber`	Sends an SMS using the phone number and SMS body specified by the `phonenumber` and `SMSBody` parameters received from the C2 server.
`Admin_ConnectedToDevice`	Sends a heartbeat message to the C2 server.

Table 1: Copybara commands and functionalities.

Conclusion

This blog analyzes the latest variants of the Copybara Android trojan that have targeted cryptocurrency exchanges and financial institutions in Italy and Spain. Through the use of logos and similar application names, the malware impersonates these institutions and lures victims into entering their credentials on phishing pages. The objective is to steal user credentials and gain unauthorized access to their accounts. However, Copybara is a fully-featured trojan that may be used in targeted attacks by malicious threat actors with powerful features such as audio & video recording, SMS hijacking, and screen capturing.

Indicators Of Compromise (IOCs)

Sample hashes

- 01b0e9cb7e864e753261b94e3e652254968d8188562a5abfc240d19fa783bc5f
- 0280536885bb406bc8cd90631bb48ddd809dcf16ecfb5acdc2e75c40171a63af
- 11470b5107f563c19ab92929a0e0ee5cf1b0c95fdd146f69ff9f9d4123f908cb
- 136efade44da726858480a9b56aab5a9509e7c04b71fec08e9b779c069632d8c
- 13b904ed2391fed303979b8b8fe0ac72a356cab091057600237fc8ac784db82a
- 1487cfbb6d702b8b2cfa88a6d586c092cdfbb472274ff54f894df35edd2f9d3e
- 19e74d9f5649e9180b2b32b95c654e7fe448d989a44c15c9b3c245fa3150df5a
- 1a3e682c924edc1dc0a525f7f1c3e2534cb2945dfaf5bad52089592d216c6c7b
- 22046aaef8a6439d1f5f2980b4d6282e7b69e98c95a0f52010d8953f0cb5e736
- 22988cbb286f387036ced6fca6bb72b9f5e326706ad99065bc04bb8cb5dc4a12
- 230f3d74004fee235055e786aba413abff2ed5cf4faa1987a070493be28c75d1
- 24a58d1168d02009c97095e75387765e63b320a0dde1f8a9a7c8e3689a3f6dfb
- 28323f93a6657363a0637341358303485d2cf240995457fc8393fb6b74f10d30
- 29e642ef6bd41f343f66210e924724bb343432affd1ed25bf386d638ae79ee87
- 2a1118c91d97a34e06344191eff546c062f81ccf58a7fa7bf1ec206a42d36c2b
- 2a5d05a6bfb3a73a91d88c15384c9b384d9309e8db0ed4e348d1a85d0f6729db
- 2d5e80f752608faa23f05e6558a695fcac261d78b9979d6746dc11dc995665e3
- 376ff4dbea2e3570a5cb98a8b335c0503d050fecd7bb4f65d252b1b596d14fc7
- 40df5d874ed86aa65454d3d7becc334b7ca2dcb11754f9131135071a98752691
- 41b61acc644add0a40ec6dbda231ae41f9de478fbf8cc029bc89d95a2829a53e
- 447c387fca23aea2b0b78f1cf9ee1c369078196fe3c3051bb99309268d4a9f79
- 472feeabc60fdcc87345574586a7599ead1625c94bf75f373e9086b4a6cfedbe
- 4b43f7145eebe4c07d208911b9d74c7c996a5037a04d52e4c38a80c2456d1187
- 4daf21a708afc06c0da4ee6e192a6db6405efb1e3a9eb6905cc69d501e781c8b
- 5bc6f1986a6e794e8feb78c763fef5f8cbb59f3696daa468aba058fb79befbf0
- 6b15d8508e6782c25dc48618bbbe9b53c8c9a822655a8e52b7370e034fae7564

- 6bc1ac4f844a6940c9e083c32bbf3f469b1322cc5aa83e12ab1a7f35cdb51c23
- 6da8e49d8e083ec705985effa03cdb60cdd736f04ed711211b2a3842c815a708
- 731a58248c7b467bc9d9a7482d8cb010242b3a534904ddc39471fa0620752d22
- 767e4c42cefc4a29921f612f14611cf56b7d950ba91ccdd3a59adb57f25b7d18
- 790b166081fd763cc6239881a78ba5c4d757b8f98d1b5d5f7abfdede76f54c05
- 7a165645df48f6bde0fd5939a3e15d160826d944e603c34d46a7285f02f0941e
- 7b3262b6c3ad52e50e2ec6faf1ffb12ca08f0d17ac4f90420f13a6053b7f9622
- 7fa3d58a0056e8492a84894a6fd3b3d0d87ff1f9656f5e54b10580b9a4a4fd6a
- 7ffbc88e97be67214ad17325142ceb54823a5bdcebdbd4e4c9d0c65b3f0a1813
- 85901707c7d058269820671e10af027eeadd39ee15f079cff340eed0f0ac9c2e
- 868ce8fa932c46b6de18455dfc0935a75029cc10c7b484bc358cdfabf0b0c533
- 878bb68727daf025c0c9619d1d12337c289489f1190410ca4025c47f39357aa5
- 8a2f6ff8aa1a6b416cb0aaa1530a8178c53760a69ce5c14d1d16ee880c335a4f
- 8b05684a73f44ed82c0faf424b2d41a0c7b00c2fef4d7dc232c5433739a59f6c
- 8bbb6cd5277177beb86b037ef77d6fcbae4a51a19668063d4d1b40ce2453dad3
- 91fda73902e1a2a76b999df11caa4532c9c440d6f3da63dc03e0a78109d7583a
- 9762eba15b893609b9461125c5adbcaf3bac7fea9536ffca72566abfa1bed084
- 9830b91dfcf987a2556afd85893f8569c6ba03e3ebb194ecb6b32dafbc22e1e1
- 989cf5faf307304f86db03180978ba4bd93c909bb458db83fcebe4fb48d7a002
- 9b204f839aed79d4c27f8d28198ef596dec9848a27a51f0672743a91e618677c
- 9c136701362e2d661805257c02e23c9aa01b9081e1a559571f947390522fc51b
- 9f693923e5641c046bdcadf10b4e2b553d078b98afc2e30f2d72660b1e0161ed
- a1a1fbdb6070ff388642974b1616d1955c2a89fbb8702caa02fa6927adbdad6c
- a46537ccf4a188091f973a47b7186ee805539a0e5d94c62867cec08cec1c33e6
- a8cc088426c6406f03ccedbb854e8dc83543d38c98a405db15074e9531731ade
- ab85b62cad1a4009bf99c621b4950ee23c413b5c424952f225497bca7a318a99
- ad1182d8bf3b1976e09f45b91085167559bc24e8f5e3f7315f96f344532cbcf8
- afa3c43141a5b6f2473d49cdfa0bce1bf0af235a40f3ec092299287291137841
- b009ad0ed336f1e4bff3f452e238b3ea83d3bc7773f52d16d057298c116a95ea
- b1b6a2d91e6fcc07322edce92aa75c13763b6844b2a1a549eeaf0f536bdc6183
- b217e4f8143a6fbbad2e0667ce8242fc207274a78ce464af9b122df8ba12690b
- b4379324c7dc1fc623bcd9d2e8099dc3588ac23f87f33151d1c1005a1f33e713
- b5c206d8f980c8fa12a29886fad49f6a1469264055740cdf763efa7f726cd8d7
- b99fc0a9eea993d6b5a04b0a0b05fe103f164fb85281fcddb04ac686daee065f
- bcae6ea26fe1dd1fa5652e05c1b888186307ad277ce238a255908061b837a484
- bff6fb5cbb1c0f8d05e2c6acefcf499a9c22f10d7db8aeda994638bf75018fbf
- c32eb3b850a20e4715a6db40635de9fc6cefad840ce7e64e9c68c2b3e378ee7e
- c8c73080a2eb18ad1434ac408e916f3f819637550dfe07f20ad79e66ec1b2cf9
- cad56908abd1508451a5af4a5304de092f0342ec6a24bbbeb9b3988683483c84
- d23ef9fe27b116d982f8ebafb99587ffc9cc6c9b932f1b2d5efab2dad156e65e
- d852f48e1c8a37d11f9dfb90f339316a5a3fa012bf152db43de1e81b45a69ba7
- d887be78f443fabeb348ac2f85e1d42ed4d1c2cfc87d9e314c4b812c0b1fcfd8
- de242d9428a378a1b0dacb2e8d481fdfb062a47450f815c13e105975d5a41663
- e097bb08da761ae5780e6c600c79738e36285a59589098dde53c88611c1ac66a
- e328dde9fa6db3da195e813696973657cc4fe636601cb0061a75c5086b04aa95
- e3875e3b20be42f38f457cf0b0d85683535472b47535635ec42da52b73b27e6e
- e57565bd3f398508321470f857dfb07c195ed9b7b494ba00dc7c407ac8b8f3e1
- e82b0023abcc4bdb549f319389620c4cbd8ffabe8648168db31db62fd84a6904
- eb1f89b2edaeda18023a6ea5cd7a4b2997e4839e1f3d57e54c5b7a1b64407874
- eb779ec4ed2c85e114a18db89b8ef9c7a19adc907748d1f18076e167f79bf04b

- f6975b1a9ab8935d45d6c2d94540b67b2374827734593c126785924afffb6634
- f703f31f7b9ef95f820a724ebcee36377e2f4a42c92756b819bea6f34ec96cac
- f91fd4f9b6594446144ba865356fde07669ea0b46a62ddd926bb8cac0aa04dc9

C2 Server IPs

- 146.103.41[.]28
- 146.19.143[.]42
- 159.100.13[.]181
- 159.100.20[.]184
- 176.124.32[.]39
- 176.126.113[.]210
- 193.3.19[.]37
- 193.31.41[.]93
- 194.99.22[.]182
- 212.237.217[.]111
- 213.109.147[.]35
- 213.109.192[.]177
- 46.249.35[.]219
- 80.251.153[.]96

Hosting URLs

- app-link[.]cc/agricole.apk
- app-token[.]cc/www.app-nueva.cc/app/BBVACodigo.apk
- aviso-clientes[.]com/www.app-nueva.cc/app/BBVACodigo.apk
- clienti-dati[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- clienti-verifica[.]com/www.app-nueva.cc/app/BBVACodigo.apk
- clienti-verifica[.]com/www.avviso-clienti[.]com/app/BNLToken.apk
- clienti-verifica[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- datos-cliente[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- datos-cliente[.]com/www.app-nueva.cc/app/BBVACodigo.apk
- datos-cliente[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- descarga-app-sign[.]com/www.avviso-clienti[.]com/app/BNLToken.apk
- descarga-app-sign[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- descargar-e-instalar[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- descargar-e-instalar[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- enlace-cliente[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- entrar-y-confirmar[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- entrar-y-confirmar[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- generali-verifica[.]com/www.app-nueva.cc/app/BBVACodigo.apk
- generali-verifica[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- generali-verifica[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- installa-app[.]com/appbnl.apk
- la-mia-app[.]com/ibl.apk
- la-mia-app[.]com/popso.apk
- la-nuova-app[.]cc/ing.apk
- scarica-app-token[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- scarica-app-token[.]com/www.avviso-clienti[.]com/app/BNLToken.apk
- scarica-app[.]icu/ZTk1ODliMTAwNTdiYjQwYjJjZDVmMDg2OTEzOTM5MWY/MyBNL.apk
- scarica-app[.]site/BNLApp.apk

- www.app-nuova[.]com/CheBancaToken.apk
- www.app-nuova[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- www.app-nuova[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- www.app-token[.]cc/www.app-nueva.cc/app/BBVACodigo.apk
- www.app-token[.]cc/www.avviso-clienti[.]com/app/BNLToken.apk
- www.descarga-app-sign[.]com/www.avviso-clienti[.]com/app/BNLToken.apk
- www.descarga-app-sign[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- www.entrar-y-confirmar[.]com/www.app-nueva.cc/app/BBVACodigo.apk
- www.entrar-y-confirmar[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- www.entrar-y-confirmar[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- www.generali-verifica[.]com/www.acceso-clientes.cc/APP/CaixaBankSignNueva.apk
- www.generali-verifica[.]com/www.app-nueva.cc/app/BBVACodigo.apk
- www.generali-verifica[.]com/www.avviso-clienti[.]com/app/BNLToken.apk
- www.generali-verifica[.]com/www.clienti-dati[.]com/App/MediobancaToken.apk
- www.generali-verifica[.]com/www.inserisci-qui[.]com/App/MedioBancaToken.apk
- www.la-nueva-aplicacion[.]com/bbva.apk