TrickMo Banking Trojan Resurgence: New Features

By cybleinc

Published: 2023-12-04 · Archived: 2026-04-06 00:10:43 UTC

Key Takeaways

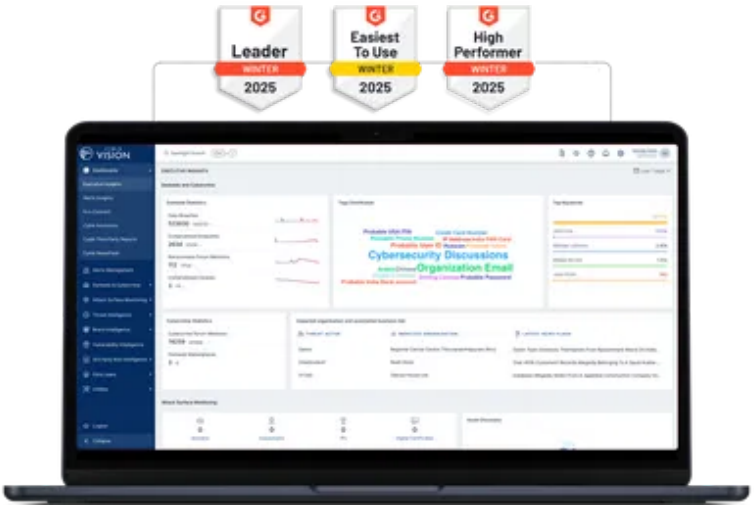
- TrickMo Banking Trojan, initially identified in September 2019, showed a resurgence in September 2023 with enhanced functionalities.
- Recent TrickMo variants use JsonPacker to conceal their code, a packing technique observed in other banking trojans.
- The latest TrickMo variant has expanded its capabilities with 45 commands, introducing features such as stealing screen content, downloading runtime modules, overlay injection techniques, and other advanced functionalities.
- This iteration of TrickMo relies on the Accessibility Service to execute Clicker and screen content exfiltration functionality.
- The malware employs an Overlay attack as the main method to harvest credentials from target applications.

Overview

The TrickMo Banking Trojan was identified in September 2019 and was disseminated through the TrickBot malware. In March 2020, IBM researchers analyzed a newly discovered Android Banking Trojan known as “TrickMo.” This Trojan specifically targeted users in Germany with the objective of stealing Transaction Authentication Numbers (TANs) by leveraging a screen recording feature.

Interestingly, Cyble Research and Intelligence Labs (CRIL) came across a new variant of this nefarious banking trojan via VirusTotal Intelligence in September 2023. This variant of TrickMo displayed enhanced functionalities upon comparison with the last documented analysis, employing overlay injection techniques to extract credentials from targeted applications instead of relying on screen recording, as observed in the first iteration.

Subsequent to the initial sample discovery, two additional TrickMo banking Trojan samples were detected on VirusTotal on October 17, 2023 (a03c968ed6f639f766cf562493a90ae7a61e909d99e098aea2abbbf607003337), and November 11, 2023 (55554c599507947c5eb96264a7db9acaa65d2b42742b39b15686836d0fac2ba0). The first of these samples masqueraded as the free movie-streaming app “OnStream,” while the other two impersonated Google Chrome.



TrickMo Banking Trojan Activity Timeline

A thorough analysis of the timeline of the TrickMo Banking Trojan's activity revealed a significant campaign spanning from 2020 through early 2021. In July 2021, a noteworthy shift occurred as the updated variant of TrickMo adopted the Overlay attack technique as its primary method for credential theft. Subsequently, from July 2021 to 2022, only six samples were identified, with two being new variants (52d4e516fe21c989cf2faf3e5ebd560c491e75cb439c5591aa3228eea64f4a73 and 493b219932c105a9e2a8dd90dbbd0bb8ffc8bab3035c7353f9beba1747ef0d4e), featuring an augmented set of 40 commands.

Following a period of inactivity, we detected three new instances of the TrickMo Banking Trojan after September 2023, as previously noted. A detailed analysis of the most recent variants revealed the incorporation of five additional commands, underscoring the continuous endeavors of the Threat Actor (TA) to improve and upgrade the malware. The depicted figure below briefly outlines the evolving timeline of TrickMo Banking Trojan's activities.

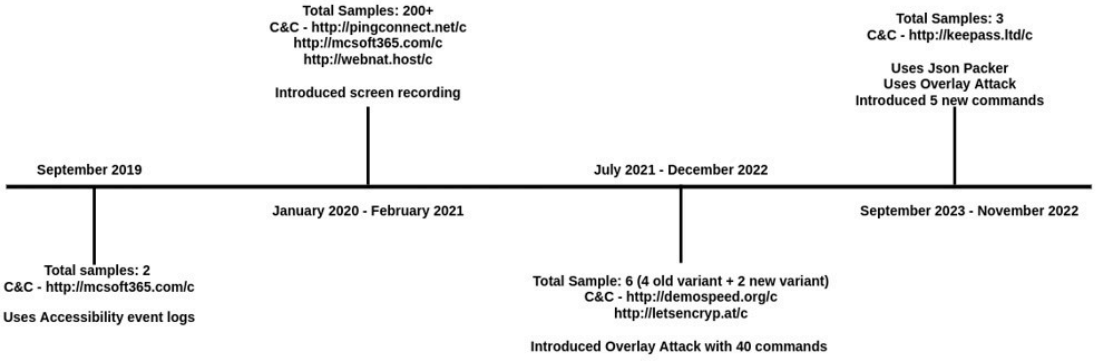


Figure 1 – TrickMo Banking Trojan Activity Timeline

Recently identified variants of the TrickMo Banking Trojan utilizing JsonPacker to conceal their malicious code. This packing technique, popular among banking trojans, has been previously observed in well-known malware like Hydra, Ermac, SOVA, and others. Notably, the malware maintains consistency in its package0020name, "d2.d2.d2," and exhibits a similar pattern in command and control (C&C) server behavior observed in previous versions. All recent samples of the TrickMo Banking Trojan establish communication with a common C&C server, specifically identified as "hxxp://keepass[.]ltd/c" and hosted on the IP address "194.169.175[.]138." Although this malicious IP

hosts Windows-related malware files, there is currently no clear evidence linking the distribution of TrickMo through these malicious files.

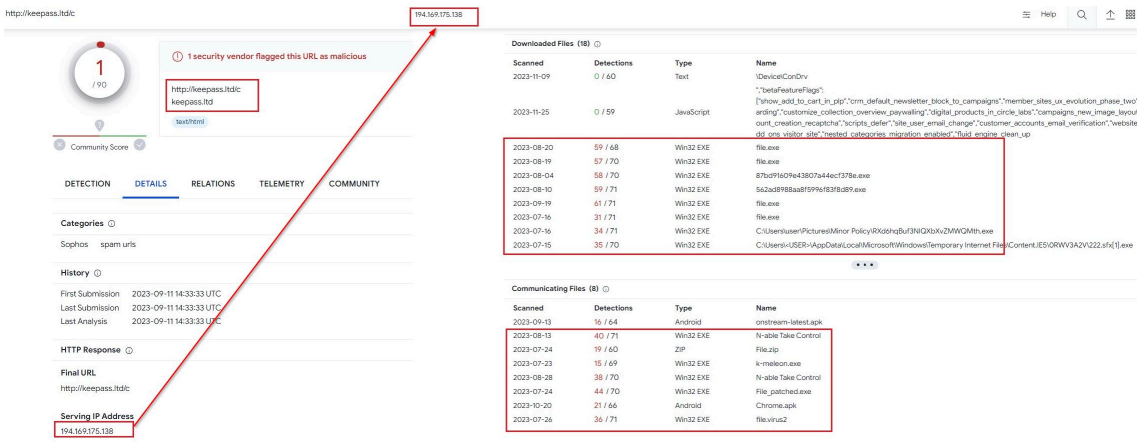


Figure 2 –Windows-based malware communicates with the IP of the C&C server

The figure below shows the admin panel of the C&C server:


Figure 3 – Admin Panel of the CC server

Figure 3 – Admin Panel of the C&C server

As explained earlier, the latest version of the TrickMo Banking Trojan has significantly expanded its arsenal, incorporating a total of 45 commands. This updated variant introduces enhanced functionalities, encompassing capabilities such as stealing screen content, the capacity to download runtime modules, overlay injection techniques, and a host of other advanced features. A comprehensive technical analysis of these additions is outlined in the subsequent section.

Technical Analysis

APK Metadata Information

- **App Name**: OnStream
- **Package Name**: d2.d2.d2
- **SHA256 Hash**: 43e19c7bbaf2d85c3952c4f28cb11ff3c711c3bb0d8396b2ac48a9d4efb955e8


Figure 4 – Application metadata information

Figure 4 – Application metadata information

Like many other widely recognized banking Trojans, TrickMo also leverages the Accessibility Service to carry out its malicious operations. Upon installation, the malware requests users to grant Accessibility permissions, which it

subsequently exploits to automatically grant further permissions and execute Banking Trojan activities.

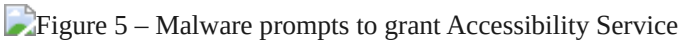


Figure 5 – Malware prompts to grant Accessibility Service

Figure 5 – Malware prompts to grant Accessibility Service

In the background, TrickMo establishes a connection with the C&C server at “hxxps://keepass[.]ltd/c” and transmits various data, including a list of installed application package name, locale, device information, Accessibility status, permission status, and other configuration details relevant to the malware.


C&C communication

Figure 6 – C&C communication

In recently observed instances of this malware posing as Google Chrome, the malware is instructed by the server to prompt users to enable the Accessibility Service. The command received by the malware includes a command ID number, along with a message and a description for the button, as illustrated in the figure below.

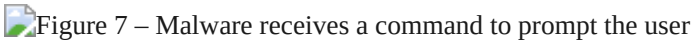


Figure 7 – Malware receives a command to prompt the user to grant Accessibility service

Figure 7 – Malware receives a command to prompt the user to grant Accessibility service

Upon obtaining permission for the Accessibility Service, the malware begins recording Accessibility logs specifically for the “com.android.settings” package. These logs are stored in a text file, named with the package name, date, and time, such as “com.android.settings_2023-11-29-07-37-14.txt”. Subsequently, these log files are compressed into a zip archive and transmitted to the C&C server.


Sending Accessibility logs

Figure 8 – Sending Accessibility logs

Overlay Attack

As previously described, the malware initially gathers the installed application’s package names to identify the target application. Upon identifying the target application, the malware then receives a command labeled “30 (SaveHtml)” accompanied by the package ID and an overlay URL. The malware proceeds to generate an HTML file on the infected device using the package ID and saves the content obtained from the provided overlay URL into this file. This HTML file will later be used as an HTML Overlay Injection page to show on the targeted application.


Malware saves HTML overlay injection pages on the infected device

Figure 9 – Malware saves HTML overlay injection pages on the infected device

Furthermore, upon establishing a connection to the Overlay URL received alongside the command, the malware is provided with a code parameter. If the code parameter is 200, the malware proceeds to load the HTML overlay injection page saved on the infected device onto the targeted application using WebView. Additionally, the malware can receive the command “11 (RequestInfo),” which includes the Overlay URL. It then loads this URL into the WebView overlay on the targeted application, allowing it to capture and steal credentials entered by the unsuspecting victim.


Malware receives a command to create an Overlay Window on targeted applications

Figure 10 – Malware receives a command to create an Overlay Window on targeted applications

A few HTML Overlay injection pages designed for various target applications are as follows:


Figure 11 – HTML Overlay injection pages

Figure 11 – HTML Overlay injection pages

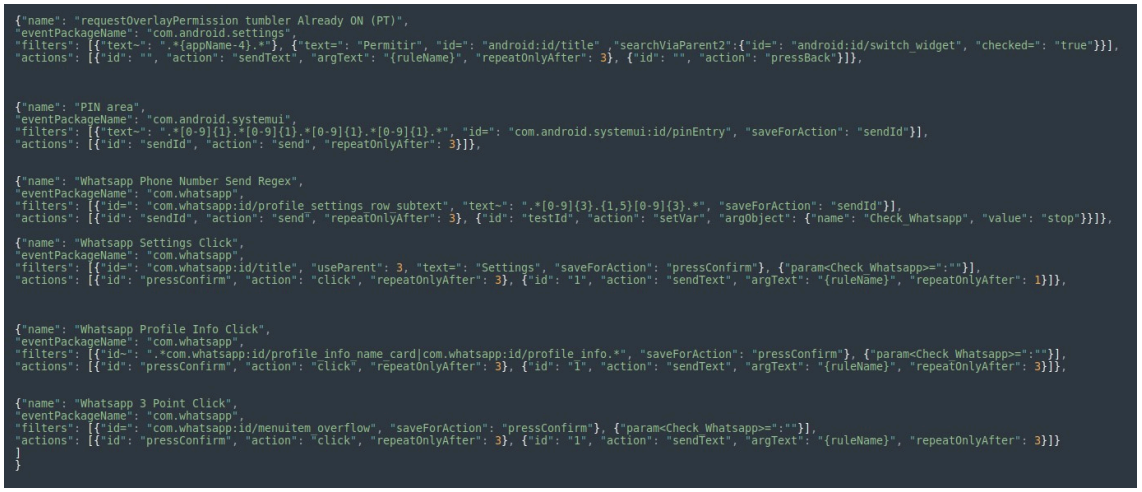
Below are a few identified targeted applications:

Application Package name	**Application name**
io.metamask	MetaMask – Blockchain Wallet
piuk.blockchain.android	Blockchain.com: Crypto Wallet
com.moneybookers.skrillpayments	Skrill – Pay & Transfer Money
com.paypal.android.p2pmobile	PayPal – Send, Shop, Manage
com.samsung.android.email.provider	Samsung Email
us.zoom.videomeetings	Zoom – One Platform to Connect
com.microsoft.office.outlook	Microsoft Outlook
com.wallet.crypto.trustapp	Trust: Crypto & Bitcoin Wallet
co.mona.android	Crypto.com – Buy BTC, ETH
com.kubi.kucoin	KuCoin: Buy Bitcoin & Crypto
com.facebook.katana	Facebook
com.okinc.okex.gp	OKX: Buy Bitcoin BTC & Crypto
com.binance.dev	Binance: Buy Bitcoin & Crypto
com.coinbase.android	Coinbase: Buy Bitcoin & Ether
com.cmcmarkets.android.cfd	CMC: Trading App
com.amazon.mShop.android.shopping	Amazon Shopping
com.ubercab.eats	Uber Eats: Food Delivery
com.ubercab	Uber – Easy affordable trips
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking
com.booking	Booking.com: Hotels and more
com.alibaba.aliexpresshd	AliExpress
com.yahoo.mobile.client.android.mail	Yahoo Mail – Organized Email

com.google.android.gm	Gmail
com.netflix.mediaclient	Netflix
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking
com.td	TD Canada
de.ingdiba.bankingapp	ING Banking to go
de.dkb.portalapp	DKB Banking
de.fiducia.smartphone.android.banking.vr	VR Banking
de.spardab.banking.privat	SpardaBanking
ae.ahb.digital	Al Hilal Digital
ca.bnc.android	National Bank of Canada
com.adcb.bank	ADCB
com.atb.ATBMobile	ATB Personal – Mobile Banking
com.bmo.mobile	BMO Mobile Banking
com.cibc.android.mobi	CIBC Mobile Banking®
com.dib.app	DIB MOBILE
com.myc3card.app	com.myc3card.app
com.fab.personalbanking	FAB Mobile

Clicker

Within the assets of the APK file, the malware includes a clicker.json file. This file contains the package names on which the auto-click functionality should operate, along with specified filters and actions to be executed on these applications.



```
{"name": "requestOverlayPermission tumbler Already ON (PT)",
"eventPackageName": "com.android.settings",
"filters": [{"text~": ".*{appName-4}.*"}, {"text=": "Permitir", "id=": "android:id/title" ,"searchViaParent2":{"id=": "android:id/switch_widget", "checked=": "true"}}],
"actions": [{"id": "", "action": "sendText", "argText": "{ruleName}", "repeatOnlyAfter": 3}, {"id": "", "action": "pressBack"}]},


{"name": "PIN area",
"eventPackageName": "com.android.systemui",
"filters": [{"text~": ".*[0-9]{1}.*[0-9]{1}.*[0-9]{1}.*[0-9]{1}.*", "id=": "com.android.systemui:id/pinEntry", "saveForAction": "sendId"}],
"actions": [{"id": "sendId", "action": "send", "repeatOnlyAfter": 3}]},


{"name": "Whatsapp Phone Number Send Regex",
"eventPackageName": "com.whatsapp",
"filters": [{"id=": "com.whatsapp:id/profile_settings_row_subtext", "text~": ".*[0-9]{3}.{1,5}[0-9]{3}.*", "saveForAction": "sendId"}],
"actions": [{"id": "sendId", "action": "send", "repeatOnlyAfter": 3}, {"id": "testId", "action": "setVar", "argObject": {"name": "Check_Whatsapp", "value": "stop"}}]},

{"name": "Whatsapp Settings Click",
"eventPackageName": "com.whatsapp",
"filters": [{"id=": "com.whatsapp:id/title", "useParent": 3, "text=": "Settings", "saveForAction": "pressConfirm"}, {"param<Check_Whatsapp>=":""}],
"actions": [{"id": "pressConfirm", "action": "click", "repeatOnlyAfter": 3}, {"id": "1", "action": "sendText", "argText": "{ruleName}", "repeatOnlyAfter": 1}]},


{"name": "Whatsapp Profile Info Click",
"eventPackageName": "com.whatsapp",
"filters": [{"id~": ".*com.whatsapp:id/profile_info_name_card|com.whatsapp:id/profile_info.*", "saveForAction": "pressConfirm"}, {"param<Check_Whatsapp>=":""}],
"actions": [{"id": "pressConfirm", "action": "click", "repeatOnlyAfter": 3}, {"id": "1", "action": "sendText", "argText": "{ruleName}", "repeatOnlyAfter": 3}]},


{"name": "Whatsapp 3 Point Click",
"eventPackageName": "com.whatsapp",
"filters": [{"id=": "com.whatsapp:id/menuitem_overflow", "saveForAction": "pressConfirm"}, {"param<Check_Whatsapp>=":""}],
"actions": [{"id": "pressConfirm", "action": "click", "repeatOnlyAfter": 3}, {"id": "1", "action": "sendText", "argText": "{ruleName}", "repeatOnlyAfter": 3}]}
]
}
```


Figure 12 – Content of Clicker.json file

The malware executes actions specified in the Clicker.json file by utilizing the Accessibility Service. With each event, the accessibility service retrieves the information from the clicker.json file, passes along event details, and subsequently performs actions based on the filters outlined in the JSON file. The malware can auto-execute any activity on the infected device without the victim's knowledge using this feature.

Figure 13 – Perform actions from the Clicker.json file

Collecting Screen Content

In earlier iterations, the malware employed the MediaProjection API to record screen content. Subsequently, the malware underwent modifications, discontinuing the screen recording functionality. Instead, the updated malware now observes running applications, captures Accessibility event logs, and saves them in a text file. This collected data is then compressed into a zip file and transmitted to the C&C server.

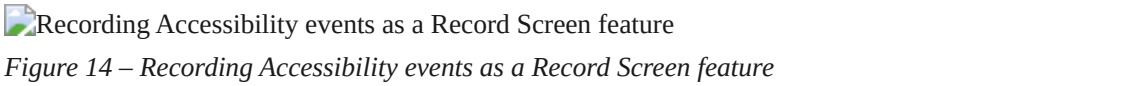


Figure 14 – Recording Accessibility events as a Record Screen feature

Moreover, upon receiving the command “15 (ScreenRecord)” along with specific package names, the malware incorporates these package names into its recording list. Subsequently, it sets the recording status to “enable”, prompting the malware to initiate the recording of Accessibility logs for the designated target applications.

```
command = "15";
if (ix.has(command)) {
   try{
      Mixer.d(String.valueOf(System.currentTimeMillis()));
      jsonObject = ix.getJSONObject(command);
      if (enable1 = params.getBoolean(str)) {
         Set apps = new ArraySet();
         JSONArray jsonArray = params.getJSONArray(jsonArray);
         int i = 0;
         while (i < jsonArray.length()) {
            command1 = packageName.toLowerCase();
            if (packageName.length() > 0) {
               apps.add(packageName);
            }
            i++;
         }
         Mixer.d(String.valueOf(System.currentTimeMillis()));
         ix1.setAppsForRecord(apps);
      }
      ix1.setEnableScreenRecord(enable);
   }catch(java.lang.Exception e0){
      ex = e0;
      Mixer.d(String.valueOf(System.currentTimeMillis()));
   }
}
```

Figure 15 – Command to receive package names to initiate Accessibility event log recording

Commands Executed By TrickMo

With each upgrade, the malware gained the ability to execute actions seamlessly without requiring user interaction. As mentioned earlier, in the latest variant, the malware introduced five new commands highlighted in the command table. These commands are designed to access application and notification settings, gather call logs, change ICON, and initiate USSD service calls.

Figure 16 – Executes USSD service call

The full list of commands executed by the malware is as follows, with the newly added commands highlighted in bold:

Command code	**Command name**	**Description**
1	Server	Set server status in shared preference
2	Interval	Get interval time for custom timer
3	DeleteAll	Receives delete all value to abort the broadcast
4	SelfDestroy	Uninstall itself
6	SetSmsApp	Set itself as the default SMS app

7	TakeScreenshot	Saves device phone number
8	SendSms	Sends SMS from the infected device
9	ShowPopup	Not Implemented
10	ActiveInterval	Sets active interval time
11	RequestInfo	Collects stolen credentials from overlay web pages
12	GetAllPhotos	Upload all photos
13	GetPhoto	Uploads single photo
14	VNC	VNC not implemented
15	ScreenRecord	Receives package name to initial recording Accessibility logs
16	LoadModule	Downloads APK
17	StartOrInstall	Launch or install a particular package
18	SetClickerConfig	Update clicker.json file
19	ShowDialog	Shows dialog box
20	ShowNotification	Displays notification
21	SetVars	Sets URL value to the iconUrl variable
22	ReadSms	Collects SMS from the infected device
23	RequestIgnoreBatteryOptimizations	Request for Battery optimization permission
24	ShowCover	Displays overlay window with the message received from the server
25	UnlockScreen	Unlocks screen
26	DisableNotifications	Disabled notification
27	PressHome	Press home button
28	PressBack	Press back button
29	OpenSetNewPasswordSettings	Open password settings
30	SaveHtml	Saves overlay phishing HTML pages
31	PressRecents	Press recent button

32	OpenPowerDialog	Opens battery optimization dialog
33	KillBackgroundProcesses	Kills running background processes
34	RequestOverlayPermission	Request to grant Display over Window permission
35	RequestPermissions	Prompts for permission
36	OpenGoogleProtectSettings	Open Google Protect settings
37	TakeScreenshot	Take screenshots of the infected device
38	Update	Update application
39	OpenAccessibilitySettings	Open Accessibility Service setting
40	GetAllVideos	Get all videos from an infected device
41	GetVideo	Get specific video
42	**OpenNotificationSettings**	Open notification settings
43	**OpenAppSettings**	Open settings application
44	**SendUssd**	Makes USSD servicel calls
45	**ReadCalls**	Collects call log
46	**ChangeIcon**	Changes ICON

Conclusion

The TrickMo Banking Trojan has demonstrated remarkable resilience and adaptability since its initial discovery in 2019, recently resurfacing in 2023 with upgraded capabilities.

The malware's transition to overlay attacks, its use of JsonPacker for code obfuscation, and its consistent behavior with the command and control server highlight the threat actor's dedication to refining their strategies. Notably, the latest variants showcase advanced features such as overlay injection techniques, clicker functionality, and the capacity to capture screen content.

Furthermore, an intriguing observation reveals the inclusion of a VNC command, though not yet implemented, suggesting that the TA is planning to introduce new features in the near future. The resurgence of TrickMo in September 2023 is a clear example of the ongoing challenges in mobile security, underscoring the need for proactive measures and heightened awareness in the face of evolving cyber threats.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Only install software from official app stores such as the Play Store or the iOS App Store.
- Using a reputed antivirus and internet security software package is recommended on connected devices, including PCs, laptops, and mobile.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Be careful while opening links received via SMS or emails sent to your mobile device.
- Google Play Protect should always be enabled on Android devices.
- Be wary of any permissions that you give an application.
- Keep devices, operating systems, and applications up to date.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Procedure
Persistence (TA0028)	Event Triggered Execution: Broadcast Receivers (T1624.001)	The malware registered broadcast receivers to trigger malicious actions.
Defense Evasion (TA0030)	Masquerading: Match Legitimate Name or Location (T1655.001)	TrickMo Masqaurades popular applications
Defense Evasion (TA0030)	Obfuscated Files or Information: Software Packing (T1406.002)	Malware uses JsonPacker
Defense Evasion (TA0030)	Download New Code at Runtime (T1407)	Malware downloads additional payload on command
Defense Evasion (TA0030)	Impair Defenses: Prevent Application Removal (T1629.001)	Abuses accessibility service to prevent uninstallation
Discovery (TA0032)	System Information Discovery (T1426)	Collects device information such as device ID, model, and manufacturer
Discovery (TA0032)	Software Discovery (T1418)	Collects installed application details
Collection (TA0035)	Input Capture: Keylogging (T1417.001)	Uses key logging feature to steal credentials
Collection (TA0035)	Data from Local System (T1533)	Collect files from storage
Collection (TA0035)	Protected User Data: SMS Messages (T1636.004)	Steals SMSs from infected device

Exfiltration (TA0036)	Exfiltration Over C2 Channel (T1646)	Sending exfiltrated data over C&C server

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
55554c599507947c5eb96264a7db9acaa65d2b42742b39b15686836d0fac2ba02b763a2f9abbb2157a9237c48d56ac985b4a8388 c74014b6ce3190c195fc2d22bfbab99e	SHA256 SHA1 MD5	TrickMo Banking Trojan file hash
hxxp://keepass[.]ltd	URL	C&C server
a03c968ed6f639f766cf562493a90ae7a61e909d99e098aea2abbbf607003337 943670e1fa503b482c38df29cc9e99c9c2cfd0f7 bef3e6f5851be75415eeb95909377af2	SHA256 SHA1 MD5	TrickMo Banking Trojan file hash
43e19c7bbaf2d85c3952c4f28cb11ff3c711c3bb0d8396b2ac48a9d4efb955e8 55e3647bb960f0faba06b39a5ddec26485f03c16 a72522b93107881ebb4651ad9258bce2	SHA256 SHA1 MD5	TrickMo Banking Trojan file hash
65d7a2019922d8c97cdc38a2b0f1bb046bf0ec35780847ac5c8fb38469e6cd58 381a8ba257c028e302d6db14170d8c000363d718 a6de677f5557816f8bddf306c81eaebc	SHA256 SHA1 MD5	TrickMo Banking Trojan Dropper file hash

---

Source: https://cyble.com/blog/trickmos-return-banking-trojan-resurgence-with-new-features/