

A rigged game: ScarCruft compromises gaming platform in a supply-chain attack

By Filip Jurčacko

Archived: 2026-06-10 02:01:13 UTC

ESET researchers uncovered a multiplatform supply-chain attack by North Korea-aligned APT group ScarCruft, targeting the Yanbian region in China – home to ethnic Koreans and a crossing point for North Korean refugees and defectors. In the attack, probably ongoing since late 2024, ScarCruft compromised Windows and Android components of a video game platform dedicated to Yanbian-themed games, trojanizing them with a backdoor.

The backdoor, named BirdCall by ESET, was originally known to target Windows only; the Android version was discovered as part of this supply-chain attack. In this blogpost, we provide an overview of the attack, and the first public analysis of the Android backdoor.

Key points of this blogpost:

- North Korea-aligned APT group ScarCruft compromised a video game platform used by ethnic Koreans living in the Yanbian region in China.
- The gaming platform's Windows client was compromised through a malicious update leading to the RokRAT backdoor, which deployed the more sophisticated BirdCall backdoor.
- Android games available on the gaming platform were trojanized to contain the Android version of the BirdCall backdoor – a new tool in ScarCruft's arsenal.
- The goal of the campaign is espionage, with the backdoor capable of collecting personal data and documents, taking screenshots, and making voice recordings.

Scarcruft profile

ScarCruft, also known as APT37 or Reaper, has been operating since at least 2012 and is [suspected to be a North Korean espionage group](#). It primarily focuses on South Korea, but other Asian countries have also been targeted. ScarCruft seems to be interested mainly in government and military organizations, and companies in various industries linked to the interests of North Korea. The group also targets North Korean defectors, with the latest such activity presented in this blogpost.

BirdCall backdoor

Windows version

BirdCall is a Windows backdoor written in C++ that we discovered in 2021 and attributed to ScarCruft as part of the [ESET Threat Intelligence](#) reporting.

The backdoor has a wide range of spying capabilities, including taking screenshots, logging keystrokes and clipboard content, stealing credentials and files, and executing shell commands. For C&C purposes, the backdoor utilizes legitimate cloud storage services, such as Dropbox or pCloud, or compromised websites. BirdCall is usually deployed in a multistage loading chain, starting with a Ruby or Python script, and containing components encrypted using a computer-specific key. The initial version of BirdCall was publicly described by South Korean vendors in 2021 as an advanced version of RokRAT ([S2W](#), [AhnLab](#)).

Android version

The Android version of BirdCall, discovered in the attack that we describe in this blogpost, implements a subset of the commands and capabilities of the Windows backdoor – it collects contacts, SMS messages, call logs, documents, media files, and private keys. It can also take screenshots and record surrounding audio.

Based on our research, Android BirdCall was actively developed over a span of several months. We identified seven versions, ranging from version 1.0 (created approximately in October 2024) to version 2.0 (created approximately in June 2025).

Discovery

Our investigation started with a suspicious APK file found on VirusTotal. Upon initial analysis, we determined that the APK is malicious and contains a backdoor.

Interestingly, the APK turned out to be a trojanized card game called 延边红十 (machine translation: Yanbian Red Ten), which we traced to its official website, [https://www.sqgame\[.\]net](https://www.sqgame[.]net). sqgame is a gaming platform tailored for the people of Yanbian and hosts traditional Yanbian games for Windows, Android, and iOS. The players can compete in card and board games (see Figure 1) with friends or join organized tournaments.



Figure 1. Yanbian Red Ten game

Surprisingly, the APK available for download on the official website is the same as the APK we initially found on VirusTotal. Moreover, a second Android game (新画图, machine translation: New Drawing) available for

download from sqgame was also trojanized with the same backdoor. Further analysis revealed that the backdoor is an Android port of the ScarCruft group's BirdCall backdoor.

The Windows desktop client link on the sqgame website leads to a few-years-old installer that appears to be clean. It does download updates once installed, but we did not identify any malicious code there during our analysis.

Investigating further in ESET telemetry, we identified a trojanized mono.dll library, originating from an update package for the desktop client. ESET telemetry shows that this update package had been malicious since at least November 2024, for an unknown period. At the time of writing, this update package was no longer malicious.

We also checked the iOS game available on the sqgame website and didn't find any malicious code. We think that ScarCruft skipped this platform, since the trojanization and delivery of the app would be much more difficult compared to other platforms, possibly running into Apple's review process.

Victimology

Since the website compromised in this attack is dedicated to the people of Yanbian and their traditional games, we infer that the primary targets are ethnic Koreans living in Yanbian. Yanbian Korean Autonomous Prefecture is a region in China that borders North Korea and is home to the largest ethnic Korean community outside Korea.

In this context, we believe that it is probable that the attack was aimed at collecting information on individuals based in (or originating from) the Yanbian region and deemed of interest to the North Korean regime – most likely refugees or defectors.

Attack overview

Android

Two of the Android games available on the sqgame website were found to be trojanized to contain the BirdCall backdoor. The download page available at [https://www.sqgame\[.\]net/games/gamedownload.aspx](https://www.sqgame[.]net/games/gamedownload.aspx) is shown in Figure 2, with download buttons for the two trojanized games highlighted in red. The third available Android game was clean at the time of our analysis.



神奇世界

www.sqgame.net

[注册](#) | [设为首页](#) | [添加到收藏夹](#)

[未成年监护](#) / [玩家社区](#) / [客服中心](#)

[首页](#) | [充值中心](#) | [下载专区](#) | [游戏商城](#) | [开通会员](#) | [游戏列表](#) | [兑奖中心](#) | [比赛排行榜](#)



神奇世界游戏大厅下载

更新时间: 2021-09-22 00:00:00
应用平台: Win2003 / WinXp / Win7 / Win10

推荐配置

- 1 CPU: 双核处理器
- 2 内存: 2GB以上
- 3 显卡: Geforce9600以上

[网通下载](#)
[电信下载](#)



新画图手机版下载





安卓版



扫二维码下载



延边麻将手机版下载





安卓版



苹果版



扫二维码下载



延边红十手机版下载





安卓版



扫二维码下载

Figure 2. Download page leading to trojanized games

We found evidence that the victims downloaded the trojanized games via a web browser on their devices and probably installed them intentionally. We have not found any other APK locations. We also have not found the malicious APKs on the official Google Play store.

We were unable to determine when the website was first compromised and the supply-chain attack started. However, based on our analysis of the deployed malware, we estimate that it happened in late 2024.

Page 4 of 18

Table 1 shows the hosting URLs of the two trojanized APK files, along with the hashes of files served at the time of discovery. At the time of writing of this blogpost, the malicious files were still up on the sqgame website. We notified sqgame of the compromise in December 2025, but haven't received a response.

Table 1. Malicious samples

Time of discovery	URL	SHA-1	Description
2025-10	http://sqgame.com[.]cn/ybht.apk	03E3ECE9F48CF4104AAF C535790CA2FB3C6B26CF	Trojanized game with the BirdCall backdoor.
2025-10	http://sqgame.com[.]cn/sqybhs.apk	FC0C691DB7E2D2BD3B0B 4C1E24D18DF72168B7D9	Trojanized game with the BirdCall backdoor.

Windows

While the Windows desktop client available on the sqgame website did not contain malicious code when we analyzed it, we later identified a trojanized mono.dll library, originating from an update package of the desktop client hosted at the URL [http://xiazai.sqgame.com\[.\]cn/dating/20240429.zip](http://xiazai.sqgame.com[.]cn/dating/20240429.zip). ESET telemetry shows that this update package had been malicious since at least November 2024, for an unknown period – but at the time of writing, this update package was no longer malicious.

ScarCruft took a clean mono library and patched it with extra code and data, containing a downloader. The downloader first checks running processes for analysis tools and virtual machine environments and does not proceed if any are found. Otherwise, it looks for the process of the sqgame client and constructs a path to the mono library in its installation folder.

Next, it downloads and executes shellcode, which contained the RokRAT backdoor at the time of discovery. Finally, the downloader terminates the client process and downloads the original clean version of the mono library, replacing the trojanized one in the installed client folder. Both the payload and clean mono library are downloaded from legitimate South Korean websites that were compromised for this purpose – a typical TTP of ScarCruft.

According to our telemetry, the RokRAT backdoor was subsequently used to download and install the BirdCall backdoor on the victimized machines.

Android BirdCall analysis

In this section, we provide a technical analysis of the Android BirdCall backdoor – an Android port of the eponymous Windows backdoor written in C++. Internally, the backdoor is named zhuagou, which can be translated (from Chinese) as “catching dogs”.

Trojanized Android games

Android BirdCall is distributed via trojanized Android games. In the attack described in this blogpost, we believe that ScarCruft did not gain access to the game's source code, only to the sqgame website or web server, and

instead took the original game APKs and recompiled or repackaged them with malicious code added.

In the trojanized APKs, the AndroidManifest.xml entry point activity is modified and points to the added malicious code – which, after starting the backdoor, executes the original entry activity of the game.

In the analyzed samples, the modified entry point activity was either `com.example.zhuagou.SplashScreen` or `com.mob.util.MobSs` (in the latest sample). The modifications to AndroidManifest.xml also include new activity and service definitions for the backdoor, as well as additional permissions required for its operation. A comparison of packages in the original game and its trojanized version is shown in Figure 3.

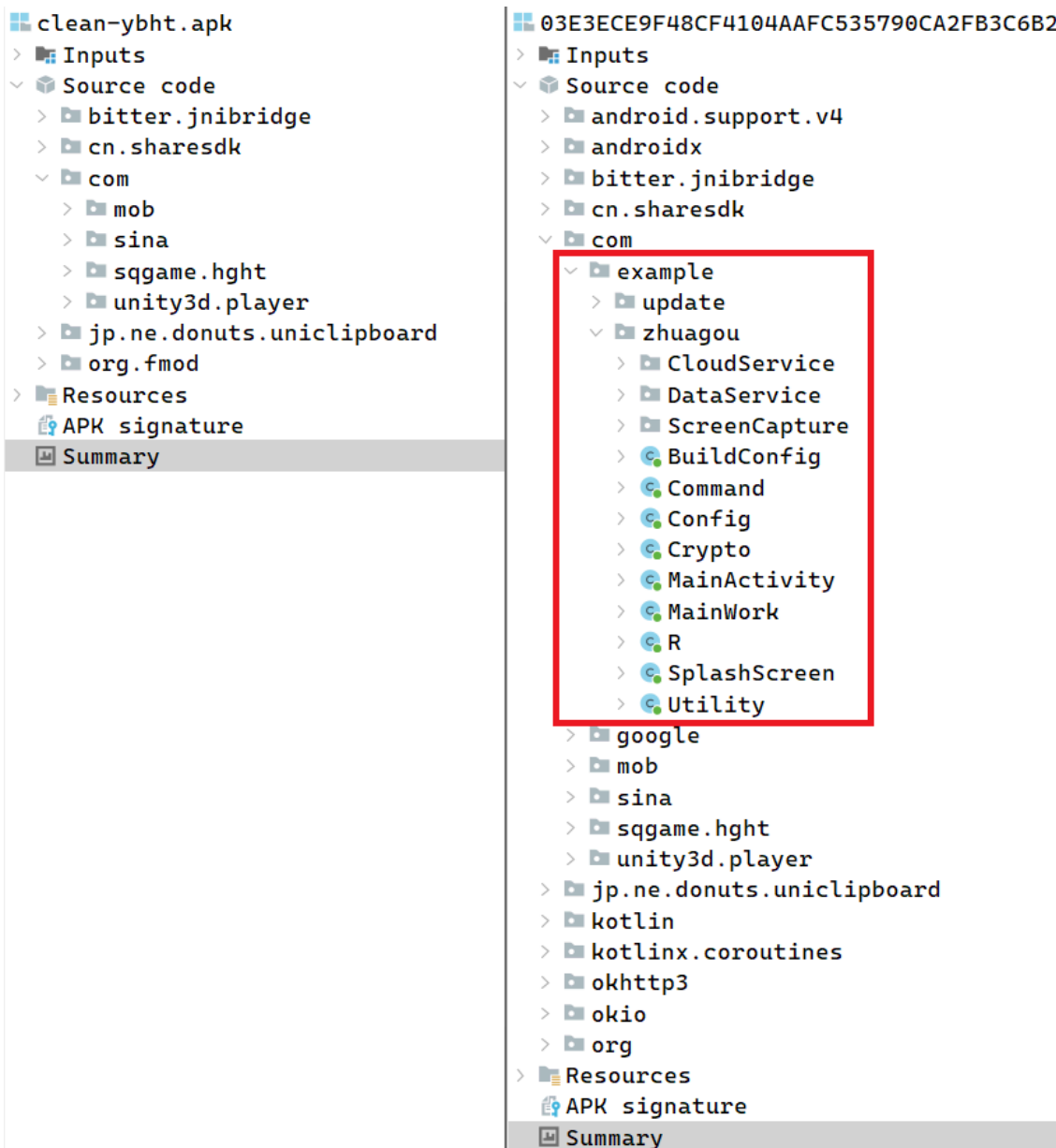


Figure 3. Package tree of the legitimate game (left) and its trojanized version (right)

Since the Android BirdCall backdoor is a part of a trojanized Android app installed on the system, it does not automatically start after installation or a device reboot; instead, it relies on user execution.

Configuration

Android BirdCall contains a default configuration, which is initialized on the first run. The configuration uses JSON format and is persisted in a file. Subsequent runs load the existing configuration file, and the configuration can be modified via backdoor commands. An example of a formatted configuration is shown in Figure 4.

```
{
  "bi": "E823D451D636D0A0",
  "skey": "A8FE823D451D636D0A0366C0629EF5C3##@((#@",
  "si": "20251105141404",
  "rft": 20000,
  "fst": true,
  "kill": false,
  "log": true,
  "ctm": 10000,
  "scr": false,
  "rec": false,
  "cmd": 0,
  "data": 1,
  "bd_version": 37,
  "extentions": ".jpg;.doc;.docx;.xls;.xlsx;.ppt;.pptx;.txt;.hwp;.pdf;.m4a;.p12;",
  "cloud": [
    {
      "ct": 9,
      "idx": 28,
      "cid": "1000.2IGB56IS1FHQ1V332R[redacted]",
      "cst": "fa7ec5c8b050[redacted]",
      "rt": "1000.a7fc479e[redacted]",
      "at": "empty",
      "fid": "8mwe5bbc0a2759839401f813968808a2f36a6",
      "dm": "",
      "use": 0
    },
    [redacted]
  ]
}
```

Figure 4. Android BirdCall configuration example

The bd_version configuration entry encodes the version of the backdoor, stored as MAJOR << 5 | MINOR, so value 37 is equal to version 1.5.

The persisted configuration file is stored in the data directory of the app and has a device-specific path. Additionally, during the configuration initialization, the default configuration of cloud storage drives hardcoded in the sample can be overridden by an external source. If available, the backdoor downloads a JPG image that

contains an encrypted cloud configuration embedded in its overlay. The image is usually hosted on a compromised South Korean website.

C&C communication

Android BirdCall uses cloud storage drives for C&C communication, similar to the Windows version. In the analyzed samples, three cloud providers are supported: pCloud, Yandex Disk, and Zoho WorkDrive, although only Zoho WorkDrive is used. The backdoor communicates via HTTPS, sending requests to API endpoints of the respective provider using the [okhttp3](#) library.

During our research, we observed 12 Zoho WorkDrive drives used by the Android BirdCall backdoor for C&C purposes. Details of the associated accounts are shown in Table 2.

Table 2. Android BirdCall Zoho WorkDrive accounts

client_id	display_name	email
1000.AJUEYDUIQQ5GCLFA68[redacted]	tomasalfred37	tomasalfred37@zohomail[.]com
1000.INXKBHQ3698CK42YA2[redacted]	kalimaxim279	kalimaxim279@zohomail[.]com
1000.FYRJ46E75TUYBWYV5J[redacted]	Smith Bentley	smithbentley0617@zohomail[.]com
1000.8QU6D2LJZ3RCGLZWF2[redacted]	Mic haelLarrow19	michaellarow19@zohomail[.]com
1000.NT1QEE7V73IHNZP5YT[redacted]	dsf sdf	amandakurth94@zohomail[.]com
1000.SKXUYYKYL06FQ2NW82[redacted]	dsf sdf	rexmedina89@zohomail[.]com
1000.7BMBOS8GV1ZR6AWEI2[redacted]	dsf dsf	alishaross751@zohomail[.]com
1000.V0J0QN7SJ2N7V6IZVE[redacted]	sdf sdf	jamesdeeds385@zohomail[.]com
1000.2IGB56IS1FHQ1V332R[redacted]	asdf sdaf	joyceluke505@zohomail[.]com
1000.W4V2XMB83C6VFC7DGZ[redacted]	dfsd sdf	marjoriemiller280@zohomail[.]com
1000.LIUBF67S89H0IZEBHE[redacted]	Bill Jackson	teresadaniels200@zohomail[.]com
1000.8BLOFSFU4WOFY9HB4A[redacted]	Zoe Jack	michaelgiesen62@zohomail[.]com

Capabilities

Android BirdCall features an update mechanism: a newer version can be loaded from an update file, which is expected to be in the form of an APK in the app data directory, and its download is triggered via the command `MP_SEND_FILE`.

After the optional update procedure, the original game activity is started, in order not to raise suspicion. Then the backdoor checks and waits for an internet connection, before proceeding to its main operation.

Data collection

On the first run, the backdoor collects a full directory listing of the device's primary [shared external storage](#), and user data consisting of contact list, call log, and SMS messages.

The backdoor periodically checks in with the C&C and uploads basic information, which consists of:

- identifier values from configuration and current time,
- battery temperature, RAM and storage information, cloud configuration, backdoor version, and file extensions of interest,
- IP geolocation information from [https://ipinfo\[.\]io/json](https://ipinfo[.]io/json), and
- on the first run, additional information about the device, network, and the application is included:
 - brand, model, OS, kernel, and rooted status,
 - IMEI number, IP address, MAC address, and network type, and
 - application package and permissions.

The backdoor can periodically take screenshots (scr flag). In some versions, we observed the technique of playing a silent MP3 file in a loop while taking screenshots, which is used to prevent the trojanized app from being suspended while running in the background.

In some of the versions, the backdoor can record audio via the microphone and eavesdrop on the surroundings of the compromised device. Strangely, even if the recording is enabled (rec flag), it is limited to a three-hour time period in the evening, from 7 pm to 10 pm local time.

The backdoor periodically searches the shared external storage for files with extensions of interest (extentions) and stages them for exfiltration. In the samples we analyzed, exfiltration was aimed at media files, documents, and private keys: .jpg, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .hwp, .pdf, .m4a, and .p12.

Commands

Android BirdCall periodically checks the cloud storage drive for commands issued for the victim. Decrypted commands start with the magic DWORD 0x2A7B4C33, and this value matches the Windows version of BirdCall. The commands have zero or more parameters, depending on their type. Table 3 shows an overview of the supported commands with their descriptions for both platforms.

The Android version of the backdoor implements only a subset of commands available in the Windows version.

Table 3. BirdCall backdoor commands

Type	Name	Android description	Windows description
0x48	MP_SET_FILESEARCH_EXTENTION	Sets file extensions of interest in the configuration.	

Type	Name	Android description	Windows description
0x49	MP_SET_THREADS	Toggles screenshot taking and voice recording.	Includes additional capabilities such as clipboard stealing and keylogging.
0x4A	MP_SET_CLOUD	Sets cloud API credentials in the configuration.	
0x4B	MP_SET_REGISTER_FILE_CONTROL	N/A	Modifies filter used during file search.
0x4C	MP_SET_MODE	Toggles collection of the backdoor execution logs.	Toggles various collection-related flags.
0x4D	MP_ACTION_KILLME	Disables the backdoor. The original game continues working.	Uninstalls the backdoor and exits.
0x4E	MP_ACTION_KILLPROCESS	N/A	Uses the taskkill utility to kill a process.
0x4F	MP_ACTION_FILE_OR_DIRECTORY	Supports upload of a specified file or directory.	Supports multiple file and directory operations: delete, rename, open, and upload.
0x50	MP_ACTION_DOWNLOAD_COMMAND	N/A	Downloads and executes commands from a URL or cloud drive.
0x51	MP_ACTION_RESET_WORKDIRECTORIES	N/A	Can delete working directories used by the backdoor.
0x52	MP_ACTION_EXECUTE_SIMPLE_COMMAND	N/A	Can restart the backdoor and execute a command via cmd.exe.
0x53	MP_ACTIONS_MORE	N/A	Can perform three operations:

Type	Name	Android description	Windows description
			· Delete persisted configuration. · Enable macros in Word (Microsoft and Hancom Office). · Restart the backdoor.
0x54	MP_ACTION_SHELL	N/A	Starts shell (based on WCMD).
0x55	MP_ACTION_WEBSCAN	N/A	Performs HTTP scan of specified hosts/ports.
0x56	MP_GET_DATA	Can obtain: · contacts, call logs, and SMS messages, · full directory listing of the primary shared external storage, and · basic information.	Can obtain: · backdoor configuration and various system information, · credentials from browsers and other software, · files from IM apps – KakaoTalk, WeChat, and Signal, · camera photos, and · directory listing.
0x57	MP_GET_TREES	Retrieves directory listing.	
0x59	MP_SEND_FILE	Supports backdoor updating.	Supports dropping of a file to a specified location, dropping and execution of additional executables, and updating of the backdoor.
0x5A	MP_SEND_SHELL	N/A	Executes shell commands.
0x5C	MP_SET_PROXY	N/A	Connects to a specified <ip>:<port> and forwards traffic from/to

Type	Name	Android description	Windows description
			the C&C server, acting as a proxy.

A dump containing the Windows version of BirdCall that closely resembles the one we observed in this attack and features all the commands listed above can be found on VirusTotal with SHA-1

B06110E0FEB7592872E380B7E3B8F77D80DD1108. The sample was uploaded from China on July 15th, 2024.

Conclusion

We have uncovered a multiplatform supply-chain attack targeting the Yanbian region through a compromised video game platform. Analyzing the trojanized Android games on the platform, we discovered a new tool in ScarCruft's arsenal – an Android version of the group's BirdCall backdoor. The Android backdoor has seen active development, and provides surveillance capabilities, such as collection of personal data and documents, taking screenshots, and making voice recordings.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in [our GitHub repository](#).

Files

SHA-1	Filename	Detection	Description
01A33066FBC6253304C9 2760916329ABD50C3191	sqybhs.apk	Android/Spy.Agent.EXM	Trojanized game with Android BirdCall version 2.0.
03E3ECE9F48CF4104AAF C535790CA2FB3C6B26CF	ybht.apk	Android/Spy.Agent.EGE	Trojanized game with Android BirdCall version 1.3.
2B81F78EC4C3F8D6CF8F 677D141C5D13C35333AF	sqybhs.apk	Android/Spy.Agent.EGE	Trojanized game with Android BirdCall version 1.5.
59A9B9D47AE36411B277 544F25AD2CC955D8DD2C	ybht.apk	Android/Spy.Agent.EGE	Trojanized game with Android BirdCall

SHA-1	Filename	Detection	Description
			version 1.0.
7356D7868C81499FB4E7 20F7C9530E5763B4C1D0	szybhs.apk	Android/Spy.Agent.EGE	Trojanized game with Android BirdCall version 1.0.
FC0C691DB7E2D2BD3B0B 4C1E24D18DF72168B7D9	szybhs.apk	Android/Spy.Agent.EGE	Trojanized game with Android BirdCall version 1.5.
95BDB94F6767A3CCE6D9 2363BBF5BC84B786BDB0	mono.dll	Win32/TrojanDownloader.Agent.ILQ	Trojanized mono library.
409C5ACAED587F62F7E2 3DA47F72C4D9EC3144D9	N/A	Win32/TrojanDownloader.Agent.ILQ	Downloader leading to the RokRAT backdoor.
B06110E0FEB7592872E3 80B7E3B8F77D80DD1108	N/A	Win64/Agent.EGN	Publicly available dump of Windows BirdCall backdoor.

Network

IP	Domain	Hosting provider	First seen	Details
39.106.249[.]68	sqgame.com[.]cn	Hangzhou Alibaba Advertising Co.,Ltd.	2024-06-01	Compromised sqgame site hosting trojanized games and malicious updates.
211.239.117[.]117	1980food.co[.]kr	Hostway IDC	2025-03-07	Compromised South Korean site used to host Android BirdCall configuration.
114.108.128[.]157	inodea[.]com	LG DACOM Corporation	2025-07-03	Compromised South Korean site used to host Android BirdCall configuration.
221.143.43[.]214	www.lawwell.co[.]kr	SK Broadband Co Ltd	2024-11-04	Compromised South Korean site used to host shellcode and clean mono library.

IP	Domain	Hosting provider	First seen	Details
222.231.2[.]20	colorncopy.co[.]kr swr.co[.]kr	LG DACOM Corporation	2025-03-18	Compromised South Korean site used to host shellcode.
222.231.2[.]23	sejonghaeun[.]com	IP Manager	2025-03-18	Compromised South Korean site used to host clean mono library.
222.231.2[.]41	cndsoft.co[.]kr	IP Manager	2025-03-18	Compromised South Korean site used to host shellcode.

MITRE ATT&CK techniques

This table was built using [version 18](#) of the MITRE ATT&CK Enterprise framework.

Tactic	ID	Name	Description
Resource Development	T1584.004	Compromise Infrastructure: Server	ScarCruft compromised South Korean websites to host payloads and configurations. ScarCruft compromised the sqgame website to perform a supply-chain attack.
	T1585.003	Establish Accounts: Cloud Accounts	ScarCruft created Zoho WorkDrive accounts and used their cloud storage drives for C&C purposes.
	T1587.001	Develop Capabilities: Malware	ScarCruft developed the Android version of the BirdCall backdoor.
	T1608.001	Stage Capabilities: Upload Malware	ScarCruft uploaded trojanized games to the compromised sqgame website.
Initial Access	T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	ScarCruft compromised an sqgame update server to distribute malicious updates.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	BirdCall can execute shell commands.

Tactic	ID	Name	Description
Defense Evasion	T1027.013	Obfuscated Files or Information: Encrypted/Encoded File	BirdCall has encrypted strings and loading chain components. The trojanized mono library contains encrypted shellcode.
	T1070.004	Indicator Removal: File Deletion	The trojanized mono library is replaced with a clean one.
	T1112	Modify Registry	BirdCall can modify settings of word processors to enable macros.
	T1140	Deobfuscate/Decode Files or Information	BirdCall decrypts strings and loading chain components.
	T1480.001	Execution Guardrails: Environmental Keying	BirdCall's loading chain has components encrypted with a computer-specific key.
	T1497	Virtualization/Sandbox Evasion	The downloader in the trojanized mono library checks for analysis tools and virtual machine environments.
Credential Access	T1555	Credentials from Password Stores	BirdCall can obtain saved passwords from browsers and other software.
Discovery	T1046	Network Service Discovery	BirdCall can scan a range of IPs and ports with an HTTP GET request.
	T1082	System Information Discovery	BirdCall can obtain various system information.
	T1083	File and Directory Discovery	BirdCall can obtain information about drives and directories.
Collection	T1005	Data from Local System	BirdCall can collect user files from IM clients KakaoTalk, WeChat, and Signal.
	T1056.001	Input Capture: Keylogging	BirdCall can log keystrokes.
	T1113	Screen Capture	BirdCall can capture screenshots.
	T1115	Clipboard Data	BirdCall can collect clipboard contents.

Tactic	ID	Name	Description
	T1119	Automated Collection	BirdCall can periodically collect files with certain extensions from local and removable drives.
	T1125	Video Capture	BirdCall can capture a webcam photo.
	T1560	Archive Collected Data	BirdCall compresses and encrypts collected data before exfiltration.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	BirdCall uses HTTP to communicate with cloud storage services.
	T1090	Proxy	BirdCall can act as a proxy.
	T1102.002	Web Service: Bidirectional Communication	BirdCall communicates with cloud storage services to download commands and exfiltrate data.
Exfiltration	T1020	Automated Exfiltration	BirdCall periodically exfiltrates collected data.
	T1041	Exfiltration Over C2 Channel	BirdCall exfiltrates data to its C&C server.
	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	BirdCall exfiltrates data to cloud storage services.

This table was built using [version 18](#) of the MITRE ATT&CK Mobile framework.

Tactic	ID	Name	Description
Initial Access	T1474.003	Supply Chain Compromise: Compromise Software Supply Chain	ScarCruft performed a supply-chain attack, compromising the sqgame website, to distribute trojanized games containing the Android BirdCall backdoor.
Defense Evasion	T1406	Obfuscated Files or Information	Version 2.0 of the Android BirdCall backdoor is obfuscated.
	T1407	Download New Code at Runtime	The Android BirdCall backdoor can download and load newer versions of itself.
	T1541	Foreground Persistence	Android BirdCall uses the startForeground API to take screenshots while in the background.

Tactic	ID	Name	Description
Discovery	T1420	File and Directory Discovery	Android BirdCall creates a directory listing and searches for files with specified extensions.
	T1422	Local Network Configuration Discovery	Android BirdCall obtains the device's IMEI, IP address, and MAC address.
	T1426	System Information Discovery	Android BirdCall obtains system information of the compromised device including brand, model, OS version, kernel version, rooted status, battery temperature, RAM, and storage information.
Collection	T1532	Archive Collected Data	Android BirdCall compresses and encrypts collected data.
	T1429	Audio Capture	Android BirdCall can record voice using the microphone.
	T1430	Location Tracking	Android BirdCall obtains approximate device location using the ipinfo[.]io service.
	T1513	Screen Capture	Android BirdCall can take screenshots.
	T1533	Data from Local System	Android BirdCall collects local files with the following extensions: .jpg, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .hwp, .pdf, .m4a, and .p12.
	T1636.002	Protected User Data: Call Log	Android BirdCall collects the call log.
	T1636.003	Protected User Data: Contact List	Android BirdCall collects the contact list.
Command and Control	T1437.001	Application Layer Protocol: Web Protocols	Android BirdCall communicates with the C&C cloud storage drive using HTTPS.
	T1481.002	Web Service: Bidirectional Communication	Android BirdCall uses a Zoho WorkDrive service cloud storage drive for C&C purposes.
Exfiltration	T1646	Exfiltration Over C2 Channel	Android BirdCall uses the C&C channel for data exfiltration.



Source: <https://www.welivesecurity.com/en/eset-research/rigged-game-scarcruft-compromises-gaming-platform-supply-chain-attack/>