

Sweet QuaDreams A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers

 citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

Bill Marczak, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, Ron Deibert

April 11, 2023

Key Findings

- Based on an analysis of samples shared with us by *Microsoft Threat Intelligence*, we developed indicators that enabled us to identify at least five civil society victims of QuaDream's spyware and exploits in North America, Central Asia, Southeast Asia, Europe, and the Middle East. Victims include journalists, political opposition figures, and an NGO worker. We are not naming the victims at this time.
- We also identify traces of a suspected iOS 14 zero-click exploit used to deploy QuaDream's spyware. The exploit was deployed as a zero-day against iOS versions 14.4 and 14.4.2, and possibly other versions. The suspected exploit, which we call **ENDOFDAYS**, appears to make use of invisible iCloud calendar invitations sent from the spyware's operator to victims.
- We performed Internet scanning to identify QuaDream servers, and in some cases were able to identify operator locations for QuaDream systems. We detected systems operated from Bulgaria, Czech Republic, Hungary, Ghana, Israel, Mexico, Romania, Singapore, United Arab Emirates (UAE), and Uzbekistan.
- QuaDream has had a partnership with a Cypriot company called InReach, with whom it is currently embroiled in a legal dispute. Numerous key individuals associated with both companies have prior connections with another surveillance vendor, Verint, as well as Israeli intelligence agencies.

1. Background: QuaDream and InReach

QuaDream

QuaDream Ltd (קוודרים בע"מ) is an Israeli company that specialises in the development and sale of advanced digital offensive technology to government clients. The company is known for its spyware marketed under the name "*Reign*", which, like NSO Group's Pegasus spyware, reportedly utilises zero-click exploits to hack into target devices.

Recent media reports indicate that QuaDream has sold its products to a range of government clients including Singapore, Saudi Arabia, Mexico, and Ghana, and has pitched its services to Indonesia and Morocco. Additionally, in their December 2022 *Threat Report on the Surveillance-for-Hire Industry*, Meta mentions that they detected activity on their

platforms that they attributed to QuaDream. The activity included the use of “about 250 accounts”, which Meta assessed were being used to test the capabilities of QuaDream’s iOS and Android spyware.

QuaDream operates with a minimal public presence, lacking a website, extensive media coverage, or social media presence. QuaDream employees have reportedly been instructed to refrain from mentioning their employer on social media. However, we have been able to identify several key figures associated with the company, including its three founders (Ilan Dabelstein, Guy Geva, and Nimrod Rinsky), through a review of corporate documentation, newspaper articles, and databases. We list these key individuals in **Appendix A**.

QuaDream is enmeshed in a legal dispute with InReach, a Cyprus-registered company. This dispute has resulted in the exposure of interesting details about the companies’ business. According to court documents obtained from the District Court of Limassol in Cyprus (the **Cypriot Case File**), QuaDream sold its products outside of Israel through InReach, a company registered in Cyprus. While the open-source information and court documents we reviewed strongly suggest that QuaDream sold its products outside of Israel through InReach, it is essential to note that this does not necessarily indicate that InReach was the exclusive or primary distributor for QuaDream.

InReach

InReach was incorporated in Cyprus in September 2017. According to assertions made by QuaDream in the Cypriot Case File, InReach was set up for the *sole* purpose of promoting QuaDream’s products outside of Israel. According to the file, a “Consortium Agreement” was signed between QuaDream and InReach on 5 July 2017, and that QuaDream took the initiative to establish the consortium in order to sell their products outside Israel. The agreement stipulated that QuaDream would receive 92% of the revenues from the sales of QuaDream’s products, with InReach keeping the remaining 8%.

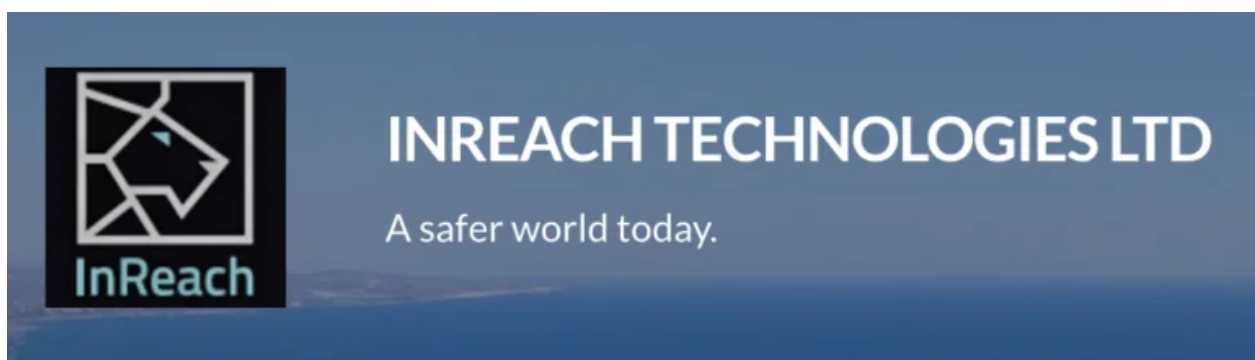


Figure 1: A screenshot from InReach’s website, [inreach\[.\]tech](http://inreach[.]tech), as captured by the Internet Archive’s Wayback Machine in August 2018.

We identify key individuals associated with InReach in **Appendix A**, through a review of corporate documents, newspaper articles, and various databases.

The Dispute Between QuaDream and InReach

One helpful source of information about QuaDream's activities is an ongoing legal dispute between QuaDream and InReach. The dispute has resulted in revelations regarding QuaDream's business practices.

The relationship between QuaDream and InReach appears to be a combination of both personal and mutual interest connections. There are notable intersections (**Appendix A**) between the two corporations and many of the key individuals from both companies seem to have former connections to Verint as well as Israeli intelligence agencies.

According to the Cypriot Case File, a dispute arose between the companies when InReach failed to transfer to QuaDream 92% of the revenues arising from sales of QuaDream's products, starting with an invoice dated 26 June 2019. On 7 May 2020, QuaDream applied to the court in Cyprus to freeze InReach's assets, pending potential arbitration in the Court of Arbitration in Amsterdam. To support their claim for a freezing order, QuaDream presented an English legal opinion which states that QuaDream is entitled to receive the sum of US\$6,079,814 from InReach (this amount presumably reflecting 92% of sales of QuaDream's products that InReach had failed to transfer, starting with the June 2019 invoice).

In the application for a freezing order, QuaDream claimed that InReach attempted to conceal and divest the assets of the consortium through fraudulent means, including by opening up a secret bank account in Switzerland and then attempting to funnel payments from customers into this new bank account, without QuaDream's knowledge. QuaDream claimed that InReach fired Lora Plotkin (**Appendix A**), a QuaDream shareholder who had signing and supervisory rights on the InReach bank account which received payments from customers, on April 17, 2020, so that InReach could funnel payments into the secret account without QuaDream's authorisation. The District Court of Limassol granted the freezing order to QuaDream and the dispute is ongoing.

2. Analysis of a Software Component Attributable to QuaDream

Microsoft Threat Intelligence shared with the Citizen Lab two samples of iOS spyware that they call *KingsPawn*, and attribute to QuaDream with high confidence. (Read the Microsoft Threat Intelligence analysis of the spyware [here](#)).

We subsequently analysed these binaries, seeking to develop indicators that could be used to identify a device compromised with QuaDream spyware. The following section describes elements of our analysis of the spyware.

Sample 1 appeared to be a downloader designed to exfiltrate basic device information, and download and execute an additional payload. **Sample 2** appeared to be a full featured spyware payload. Nevertheless, both **Sample 1** and **Sample 2** shared highly distinctive

commonalities, including largely identical functions for spawning processes. The functions create (and later remove) a distinctive subfolder within the **com.apple.xpc.roleaccountd.staging** folder on the phone:

```
/private/var/db/com.apple.xpc.roleaccountd.staging/PlugIns/fud.appex/
```

Additionally, both **Sample 1** and **Sample 2** parse the same distinctive JSON encoding of 40 kernel memory offsets that provide the location of various iOS kernel structures presumably important for the spyware's operation. We suspect that this encoding is generated by an earlier stage in the exploit chain, and passed to **Samples 1** and **2**.

In addition to the high-confidence attribution by *Microsoft Threat Intelligence* to QuaDream, we found several references linkable to QuaDream in **Sample 1**. The second sample, **Sample 2**, did not contain these references.

Functionality

Sample 1 appeared to be an initial payload whose purpose was to download another payload. **Sample 2**, however, appeared to be the final spyware payload. Our analysis of **Sample 2** allowed us to identify a range of functionality that helps the implant perform its core surveillance capabilities. Like other, similar, mercenary spyware the implant has a range of capabilities from hot-mic audio recording of calls and the environment, to more advanced capabilities to search through the phone.

QUADREAM FUNCTIONALITY









-  Record audio from calls
-  Record from the microphone (“hot mic”)
-  Take pictures using front & back cameras
-  Exfiltrate and remove keychain items
-  Generate iCloud 2FA passwords
-  Search through device files & databases
-  Clean up its own traces
-  Track location

Figure 2: Spyware functionality we identified in Sample 2.

Sample 2 appears to have functionality for:

- Recording audio from phone calls
- Recording audio from the microphone
- Taking pictures through the device’s front or back camera
- Exfiltrating and removing items from the device’s keychain
- Hijacking the phone’s *Anisette* framework and hooking the *gettimeofday* syscall to generate iCloud time-based one-time password (TOTP) login codes for arbitrary dates. We suspect that this is used to generate two-factor authentication codes valid for future dates, in order to facilitate persistent exfiltration of the user’s data directly from iCloud
- Running queries in SQL databases on the phone
- Cleaning remnants that might be left behind by zero-click exploits
- Tracking the device’s location
- Performing various filesystem operations including searching for files matching specified characteristics

We found that the spyware also contains a self-destruct feature that cleans up various traces left behind by the spyware itself. Our analysis of the self-destruct feature revealed a process name used by the spyware, which we discovered on victim devices.

QuaDream Spyware Process Name Emerges

A function in **Sample 2** hard-codes the path to the main spyware payload (in a XOR-obfuscated string) as */private/var/db/com.apple.xpc.roleaccountd.staging/subbridged*. While *subbridged* is the name of a legitimate iOS executable, the legitimate *subbridged* would not be launched from the */private/var/db/com.apple.xpc.roleaccountd.staging/* directory. This process name has never been observed used by NSO Group's Pegasus spyware (which also uses the */private/var/db/com.apple.xpc.roleaccountd.staging/* directory), nor any other type of spyware of which we are aware.

Another function in **Sample 2** removes entries from the */private/var/root/Library/Caches/locationd/clients.plist* file, which is a well-publicised forensic source where spyware indicators may persist. The function attempts to remove entries ending in the string "subbridged" from this file.

Cleanup Code Highlights Suspected Zero-Click Exploits

We identified functionality within **Sample 2** that deletes events from the iOS calendar. The functionality is located in two "Calendar Cleanup Functions", which we refer to as **CCF1** and **CCF2**. The functions appear to be executed when a special cleanup command is received from the spyware's command-and-control server. The cleanup command includes an email address that specifies the scope of the cleanup.

CCF1 enumerates (via EventKit) all calendar events in all calendars whose start date is after 728 days ago, and checks whether the email address of the event's organiser is equal to the supplied email address. If so, then the event is removed via the *-[EKEventStore removeEvent:span:commit:error:]* function.

CCF2 opens the SQLite database that stores calendar information on the phone, located at */var/mobile/Library/Calendar/Calendar.sqlitedb*, using the following parameters:

```
file:%s?cache=shared&mode=rwc&_journal_mode=WAL&_timeout=10000
```

CCF2 then checks to see if the supplied email address is present in the 'Participant' table in the database:

```
SELECT DISTINCT identity_id FROM Participant WHERE email = "%s"
```

If present, then these deletion queries are run:

```
DELETE FROM Identity WHERE ROWID = %d;
DELETE FROM CalendarItemChanges WHERE record IN ( SELECT owner_id FROM
ParticipantChanges WHERE email = "%[2]s" );
DELETE FROM ParticipantChanges WHERE email = "%[2]s";
```

Finally, **CCF2** vacuums the database:

```
VACUUM;
PRAGMA wal_checkpoint(TRUNCATE);
```

The same cleanup command that triggers deletion of calendar events associated with a specific email address also causes that same email address to be removed from the `com.apple.identityservices.idstatuscache.plist` file (in `/private/var/mobile/Library/Preferences/`). In iOS versions 14.6 and prior, this file contained a record of iCloud accounts that the device had interacted with using certain Apple services (e.g., iMessage). This file appears to have been deprecated since iOS version 14.7, and no longer stores any information.

The *Ectoplasm Factor*

We noted functionality within **Sample 2** that sometimes leaves traces behind on infected devices after the spyware is removed. We refer to these traces as the ***Ectoplasm Factor***. We omit discussion of the ***Ectoplasm Factor*** from our report, as we believe this may be useful for tracking QuaDream's spyware going forward.

Exfiltration

The spyware exfiltrates data via HTTPS POST requests. The spyware's exfiltration module appears to have the capability to use a custom root certificate for this HTTPS connection, indicating that exfiltration may involve self-signed certificates. Separately, we observed suspected QuaDream exfiltration to servers returning self-signed Kubernetes certificates.

3. Target Forensics

We uncovered clues that we believe are linked to QuaDream's iOS 14 zero-click exploit. While NSO Group was deploying ***FORCEDENTRY*** as a zero-click, zero-day exploit against iOS 14 devices, QuaDream appears to have been deploying a separate zero-click, zero-day exploit against iOS 14 devices that we refer to as ***ENDOFDAYS***. Apple reportedly notified targets of both Pegasus and QuaDream hacking in a round of notifications issued on 23 November 2021.

We shared our analysis of this attack with Apple Inc. at multiple points during our investigation.

ENDOFDAYS, a Possible Zero-Click Exploit

We identified two 2021 cases where targets in North America and Central Asia showed evidence that a process named ***/private/var/db/com.apple.xpc.roleaccountd.staging/subridged*** had run on the phone on iOS versions 14.4 and 14.4.2, while these were the latest iOS versions.

In one case, we were able to examine the user's Calendar.sqlitedb file, and also connect (via CalDAV) to their iCloud calendar. The user's Calendar.sqlitedb file showed a suspicious event added to the calendar in 2021 organised by a user **[REDACTED1]@icloud.com**. The summary of the event was "Meeting", and the description of the event was "Notes". We obtained an .ics file for this event from their iCloud calendar via CalDAV. The event contained remnants of a possible XML escape, where the CDATA opening and closing tags were embedded in keys in the .ics file (highlighted below).

```
DESCRIPTION ]]> :x
ATTENDEE;EMAIL=[redacted victim]...
ATTENDEE <![CDATA[ :Notes
```

We located a second .ics file for an event added in 2021 containing the same summary and description, and the same possible XML injection, but organised by a different user **[REDACTED2]@icloud.com**. Details of this event and organiser did *not* appear in the user's Calendar.sqlitedb file, and may have been deleted by the spyware.

We suspect that the attacker's use of closing and opening CDATA tags in the .ics could potentially facilitate the inclusion of additional XML data that would be processed by the user's phone, in order to trigger some behaviour desired by the attacker. When a user is invited to an iCloud calendar event, APNs (the Apple Push Notification Service) delivers a message with topic *com.me.cal* to the user's devices. The message comprises the user's DSID (Directory Services Identifier). This message is routed to the iPhone's *dataaccessd* process, causing it to perform a WebDAV sync (RFC 6578) with the iCloud calendar server to obtain a list of URLs of new calendar events to fetch. The *dataaccessd* process then supplies these URLs back to the iCloud calendar server in a *CALDAV:calendar-multiget REPORT* (RFC 4791), and the server responds with each file's iCalendar data embedded within CDATA tags in a calendar-data XML element.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<multistatus xmlns="DAV:">
<response xmlns="DAV:">
  <href>/path/to/event.ics</href>
  <propstat>
    <prop>
      <getetag xmlns="DAV:">"..."</getetag>
      <calendar-data xmlns="urn:iETF:params:xml:ns:caldav">
        <![CDATA[BEGIN:VCALENDAR
          ...
```


Thus, the attacker's use of closing and opening CDATA tags in the .ics could potentially allow them to inject XML data that would be processed by the user's phone into the response. While we were not able to recover any XML data from the .ics files, these files appear to have been updated once, judging by the SEQUENCE and LAST-MODIFIED fields.

A Signature for *ENDOFDAYS*

All of the calendar events we identified used as part of the *ENDOFDAYS* attack can be detected by running the following query on a phone's Calendar.sqlitedb file.

```
SELECT * FROM calendaritem WHERE summary="Meeting" AND description="Notes";
```

The malicious calendar events have additional distinctive characteristics that appear to always be the same. The .ics file contains invitations to *two overlapping events* that are *backdated*. On iOS 14, any iCloud calendar invitation with a backdated time received by the phone is automatically processed and added to the user's calendar with no user-facing prompt or notification. We are unsure why the events are overlapping, though there may be a specific behaviour triggered by overlapping events.

We examined Calendar.sqlitedb files from two phones which showed the */private/var/db/com.apple.xpc.roleaccountd.staging/subridged* process name in 2019 and 2020. Overall, we have not observed any *ENDOFDAYS* calendar events generated prior to January 2021, leading us to believe that *ENDOFDAYS* was targeted at iOS 14.

Other Observations about *ENDOFDAYS*

At least one target who was notified by Apple tested positive for QuaDream's spyware and was negative for Pegasus.

We have not observed any cases of individuals targeted with *ENDOFDAYS* prior to January 2021 or after November 2021.

We have also observed evidence of infections where the QuaDream spyware payload was customised. In one case, we found indications that the phone's *duetexpertd* process was somehow coaxed to launch a WebKit instance, which may have been induced to navigate to a malicious URL, leading to further exploitation, and the execution of the spyware.

Summary of Target Forensics

Overall, we identified at least five targets showing indicators of infection or targeting with QuaDream's spyware or exploits. We attribute two cases to QuaDream's spyware or exploits with high confidence, as they match multiple QuaDream indicators, and three with medium confidence, as they only match a single indicator.

Case	Evidence that Supports QuaDream Infection	Timeframe	Confidence
C1	<i>subridged</i> run from <i>com.apple.xpc.roleaccountd.staging</i>	Unknown	Medium
C2	<i>subridged</i> run from <i>com.apple.xpc.roleaccountd.staging</i>	2019	Medium
C3	<i>subridged</i> run from <i>com.apple.xpc.roleaccountd.staging</i>	2019, 2020	Medium
C4	<ul style="list-style-type: none"> • ENDOFDAYS calendar events • <i>subridged</i> run from <i>com.apple.xpc.roleaccountd.staging</i> • Ectoplasm Factor 	2021	High
C5	<ul style="list-style-type: none"> • <i>subridged</i> run from <i>com.apple.xpc.roleaccountd.staging</i> • Ectoplasm Factor 	2021	High

4. Internet Scanning for QuaDream Servers

Partners in the threat intelligence community shared a network indicator linked to QuaDream’s spyware with us. Pivoting off of this indicator, we were able to devise fingerprints and identify more than 600 servers and 200 domain names that we conclude with high confidence were linked to QuaDream’s spyware between late 2021 and early 2023, including servers that we believe are used to receive data exfiltrated from QuaDream victims, and servers used for QuaDream’s one-click browser exploits.



Figure 3: Suspected locations of QuaDream operators.

In several cases, we were able to trace these servers back to their operators. We believe that there are QuaDream systems operated from the following countries:

- Bulgaria
- Czech Republic
- Hungary
- Ghana
- Israel
- Mexico
- Romania
- Singapore
- United Arab Emirates (UAE)
- Uzbekistan

We shared our results with Microsoft Threat Intelligence, who conducted additional scanning to identify QuaDream-linked domain names. Microsoft Threat Intelligence are publishing the results of their scanning in [their report](#).

Countries of Concern

Hungary, Mexico, and the United Arab Emirates are known to abuse spyware to target human rights defenders (HRDs), journalists, and other members of civil society. The Citizen Lab has [reported extensively](#) on spyware abuse in Mexico. A [report](#) published in March 2023 by Mexican digital rights organisation R3D uncovered evidence that Mexico's Army was behind some of this surveillance abuse. The Citizen Lab has also reported extensively on the

UAE Government's abuse of spyware to target HRDs, intellectuals and activists. The *Pegasus Project* uncovered evidence suggesting that Hungary's government was behind the abusive use of spyware to target Hungarian journalists, and the Citizen Lab verified that Hungarian photojournalist Dániel Németh's phone was infected with Pegasus.

We cannot determine if the systems operated from Israel are operated by the Israeli government or QuaDream itself. Nevertheless, the Israeli government is also suspected to have abused mercenary spyware to target Palestinian HRDs, as well as domestic political activists.

Additionally, several other countries are known to have deficiencies in surveillance oversight, or otherwise poor human rights records. Uzbekistan has a long record of serious human rights violations, and the regime imposes significant restrictions on basic human rights, including freedom of expression, association, and peaceful assembly. Singapore's constitution does not recognize the right to privacy, and state authorities have broad surveillance powers that bypass standard judicial mechanisms.

5. Request for Comment

On April 7, 2022, the Citizen Lab sent an email to Vibeke Dank, who is listed as QuaDream's legal counsel, asking questions about how QuaDream's business practices take into account human rights and the potential for spyware abuse, and inviting comment on the locations of suspected operators we identify in our report. We received no response as of the date of publication of this report.

6. Conclusion

QuaDream's obscurity reflects an effort to avoid media scrutiny that was successful, for a time. Yet once QuaDream infections become discoverable through technical methods, a predictable cast of victims emerged: civil society and journalists. This pattern is a repetition of the abuses found with more notorious players, like NSO Group's Pegasus spyware, Cytrox's Predator spyware, and before them Hacking Team and FinFisher.

QuaDream has been in business for several years, has developed sophisticated spyware products, and appears to have dealings with numerous government clients around the world. The firm has common roots with NSO Group, as well as other companies in the Israeli commercial spyware industry, and the Israeli government's own intelligence agencies.

Like NSO Group, Intellexa, and other commercial spyware firms we have studied, QuaDream employs complicated and opaque corporate practices that may be designed to evade public scrutiny and accountability. For example, it appears that its troubled partnership with InReach may have been designed as a way to evade export controls and government

oversight. Such convoluted corporate structures impair accountability by impeding investigations and making it difficult to ensure that companies are operating in compliance with applicable laws and regulations.

Ultimately, this report is a reminder that the industry for mercenary spyware is larger than any one company, and that continued vigilance is required by researchers and potential targets alike. Until the out-of-control proliferation of commercial spyware is successfully curtailed through systemic government regulations, the number of abuse cases is likely to continue to grow, fueled both by companies with recognizable names, as well as others still operating in the shadows.

Appendix A: Key Individuals at QuaDream and InReach

We have identified key individuals associated with QuaDream and InReach through a review of corporate documents, newspaper articles, and various databases.

Key Individuals at QuaDream

- **Ilan Dabelstein:** Dabelstein is a former Israeli military official who holds a significant position in QuaDream as a co-founder, major shareholder, and board member. Corporate registration documents in Israel dated February 17, 2021 indicated that he held the position of CEO. According to a June 22, 2022, report by *Intelligence Online*, Ilan Dabelstein is the only founding member still holding shares in QuaDream.
- **Guy Geva and Nimrod Rinsky:** According to documents obtained from Israel's corporate register, Geva and Rinsky are co-founders and significant shareholders in QuaDream who, according to *Reuters*, both previously worked for NSO Group. Although the latest documents we obtained from Israel's corporate register show Geva and Rinsky are shareholders in QuaDream, *Intelligence Online* reported that both men sold their shares in the company in early 2022.
- **Vibeke Dank:** According to Israeli corporate registration documents, Dank is a lawyer who has been granted authority to sign legal documents on behalf of QuaDream. *Reuters* noted that Dank's email address was listed on QuaDream's corporate registration form. A recent *IntelligenceOnline* [report](#) pointed to Dank's role in providing legal assistance to mercenary spyware vendors, such as NSO Group, QuaDream, and NFV Systems, which were [sanctioned](#) by the Israeli Defense Ministry in March 2023.

- **Avi Rabinowitz/Avi Rabinovitch:** Rabinowitz (or Rabinovitch) is a key principal and CEO at QuaDream according to [DNB](#) and [Haaretz](#). He was also described by QuaDream in the Cypriot Case File as QuaDream’s “sales manager.” According to his [LinkedIn profile](#), he served as an Executive VP of sales of a “Cyber Startup” between November 2018 to May 2021, “CEO” from June 2021 to January 2023, and as of January 2023, he has been “Cooking New Things.” Prior to working at QuaDream, Rabinovitch co-founded a company called Mabaya which was later sold to the NASDAQ listed company, Criteo. Prior to this, he worked for Verint in a sales role for over 8 years.
- **Zvi Fischler:** In November 2019, [Intelligence Online](#) reported that Fischler “was QuaDream’s head of sales for a long time.” According to his [LinkedIn](#), Fischler was an officer in the elite intelligence unit in the Israeli military for 16 years (1973-1989). Following that period, he spent 22 years at Verint (1993-2015) in sales and marketing for the EMEA region. In January 2019, he listed himself as a self-employed “sales specialist.” Fischler and Rabinovitch are connected on LinkedIn, with the latter having “endorsed” the former in “telecommunication” skills.
- **Lora Plotkin:** Plotkin is a former shareholder of QuaDream and a former finance manager at InReach.
- **Uri Ashkenazi:** [Intelligence Online](#) reported in July 2022 that Ashkenazi was building up his interests in Israeli cyber intelligence and acquired shares in QuaDream. He is also one of the main shareholders of [D&W Ventures](#) which holds a substantial stake in QuaDream. Ashkenazi, as [reports](#) describe him, is an Israeli financier who is increasingly investing in Israel’s cyber intelligence sector. His [LinkedIn](#) profile states that he is the Managing Partner of Titan Ventures, a venture capital fund that invests in early stage startups, with a focus on disruptive software solutions for the cyber intelligence and defence industries. He is also an investor in other companies such as [Cobwebs](#) and [Falkor](#).

Key Individuals at InReach

- **Roy Glasberg Keller:** The articles of incorporation of InReach identify Cycotech Ltd. as the sole owner of InReach with 1000 shares. Cycotech was incorporated in Cyprus on August 31, 2017. It was originally registered under the name “Zovisel” but then changed its name to Cycotech shortly after. Cycotech’s articles of incorporation indicate that Roy Glasberg Keller, an Israeli businessman living in America, is the sole shareholder with 1000 shares. This makes Keller the sole shareholder of InReach. According to his [LinkedIn](#) profile, Keller is based in Los Angeles, California. He is the CTO of Prelude Communications and [describes](#) himself on LinkedIn as having:

spent his carrier [sic] advancing cyber and information security from service in the Israeli Air Force to a US vice president and a senior strategic advisor at Verint (NASDAQ:VRNT) a world leader in actionable intelligence. Roy lead [sic] teams in support of US and NATO forces in the war on terror in operational assessment and in the field. Roy also supports the correction industry ongoing effort to defeat the cell phones in correction facilities both in the US and internationally [sic].

He appears to have served in the Israeli Air Force between 1992 and 1999 and held the position of CEO of U-TX between 2007 and 2014. After U-TX was acquired by Verint, he became the CEO of U-TX for a year and then served for one more year as a VP senior strategic advisor at Verint. His time at Verint overlapped with Fischler.

- **Doron Breiter, Christos Shiakallis, and Nenad Grozdanic:** Breiter, Shiakallis, and Grozdanic are the three founders of InReach. Grozdanic is the company’s chief information officer (CIO). The three founders were previously with U-TX Technologies. U-TX was acquired by Verint in 2014 for \$83 million. While [media reports](#) suggest that Shiakallis and Grozdanic are the owners of InReach, the corporate documents we obtained from the Cypriot company register show that Cycotech Ltd. is the sole owner.
- **Doron Breiter:** Reports from [Intelligence Online](#) identify him as one of the founders of InReach. His [LinkedIn](#) profile indicates that he is currently residing in Cyprus and holds two current roles, one as a “consultant at a startup in stealth mode” and the other as a “Co-Founder of Confidential.” He also appears to have professional connections with Verint. He filed four [patent applications](#) related to IMSI products with Verint in 2015, 2017, and 2019. Moreover, a recent patent [application](#) filed in the US in 2020 suggests that he may also have ties to the Israeli company [Cognyte](#).
- **Christos Shiakallis:** Shiakallis is one of the founders of InReach. He completed his MBA at the Kellogg School of Management in Illinois, like Breiter and Keller. According to his [LinkedIn](#) profile, he is based in Dubai, UAE, and similar to Breiter, since July 2018 to date, he has been a consultant at “start-up in stealth mode” and a “co-founder in confidential.”
- **Nenad Grozdanic:** According to [Intelligence Online](#), Nenad is one of the founders of InReach. The Cypriot Case File describes him as the company’s General Manager and Chief Information Officer. According to his [LinkedIn](#) page, Nenad is based in Dubai and is a “senior systems architect at confidential.”

- **Lora Plotkin:** Along with being a former shareholder of QuaDream, according to the Cypriot Case File, Plotkin is also the former finance manager at InReach. QuaDream claims in the Cyprus proceedings that she was the method by which QuaDream exercised oversight of InReach’s finances. Plotkin is a member of a Facebook group called “Questions and Answers – Help for startups.” In July 2017, three months before the agreement with InReach was signed, she posted a message on the group asking to consult with an expert on “indirect” exporting.



Lora Plotkin

27 July 2017 · 🌐



היי קבוצה יקרה. האם יש פה מומחה להתייעץ איתו לגבי מפעל מעודף ויצואן עקיף? תודה!

Hi dear group. Is there an expert here to consult with about a surplus factory and indirect exporter? Thank you!

⚙️ · [Hide Translation](#) · [Rate this translation](#)

- **Savvas Angelides and Christos Ioannides:** A.I.L Nominee Services Ltd (A.I.L) are listed as InReach’s director and secretary in corporate filings obtained from Cyprus (the company is also the director and secretary of Cycotech). A.I.L was registered in Cyprus on 27 July 2010 and states its principal activities as “business, management and consultancy services.” Savvas Angelides was a founding shareholder in A.I.L. Angelides is the current Deputy Attorney General and former Minister of Defence of Cyprus. He transferred his shares in A.I.L. to Christos Ioannides on 16 February 2018 and was appointed Minister of Defence on 1 March 2018. On 29 June 2020, he was appointed Deputy Attorney General. Ioannides remains the only shareholder of A.I.L.

Acknowledgements

We are especially grateful to the victims and suspected targets in this investigation. Although they are not named in this initial report, without their willingness to share materials for analysis, this report would not have been possible.

We are grateful to Adam Senft and Snigdha Basu for editorial assistance, and Mari Zhou for graphical work on this report.

Special thanks to Access Now, especially the Digital Security Helpline.

Special thanks to Microsoft Threat Intelligence for sharing samples, and Censys.

Special thanks to TNG and CQ.