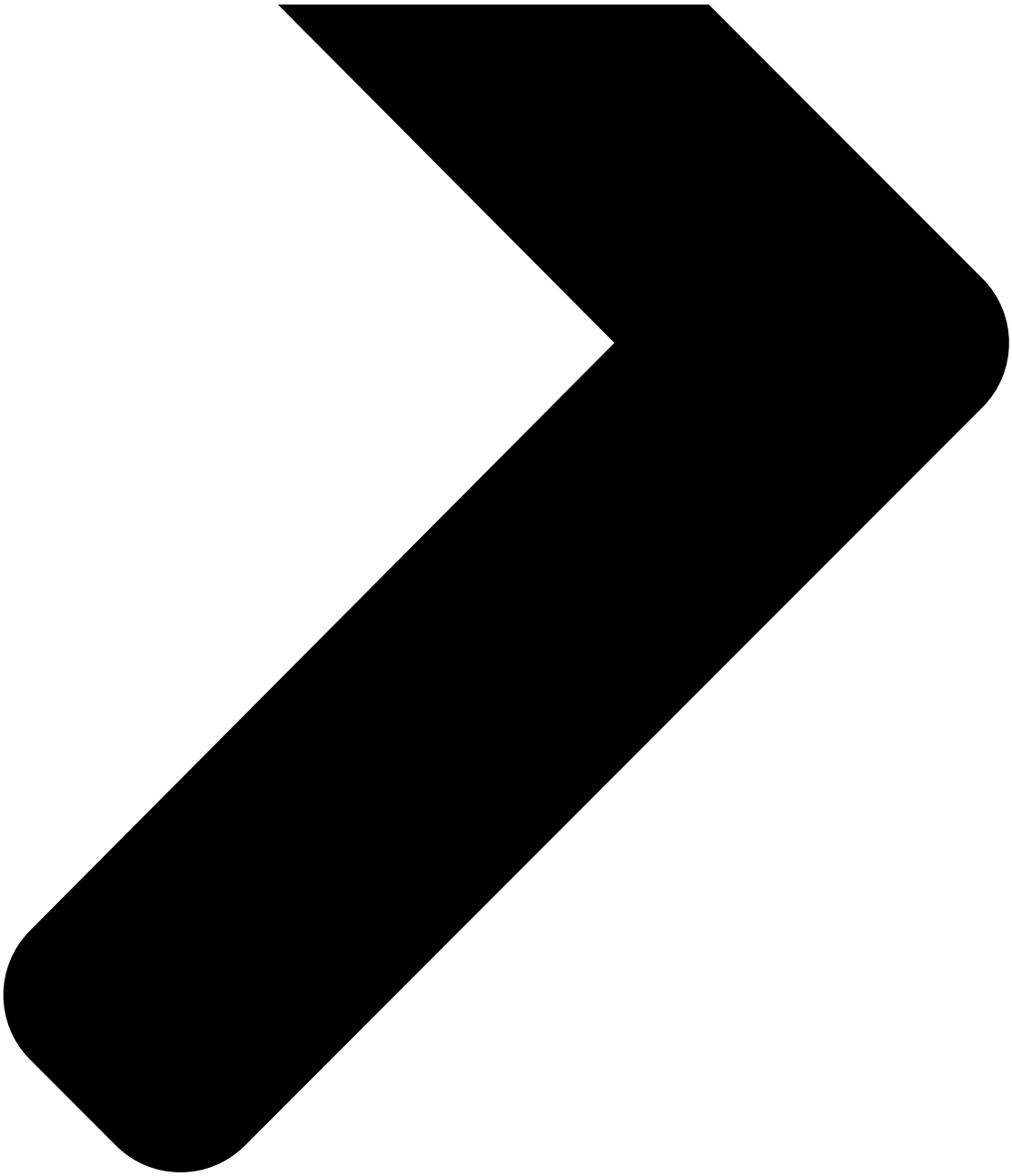
# Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus

citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

July 15, 2021

Research



Targeted Threats

By Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert

July 15, 2021

## Summary


- Candiru is a secretive Israel-based company that sells spyware exclusively to governments. Reportedly, their spyware can infect and monitor iPhones, Androids, Macs, PCs, and cloud accounts.
- Using Internet scanning we identified more than 750 websites linked to Candiru's spyware infrastructure. We found many domains masquerading as advocacy organizations such as Amnesty International, the Black Lives Matter movement, as well as media companies, and other civil-society themed entities.
- We identified a politically active victim in Western Europe and recovered a copy of Candiru's Windows spyware.

- Working with Microsoft Threat Intelligence Center (MSTIC) we analyzed the spyware, resulting in the discovery of **CVE-2021-31979** and **CVE-2021-33771** by Microsoft, two privilege escalation vulnerabilities exploited by Candiru. Microsoft patched both vulnerabilities on July 13th, 2021.
- As part of their investigation, Microsoft observed at least 100 victims in Palestine, Israel, Iran, Lebanon, Yemen, Spain, United Kingdom, Turkey, Armenia, and Singapore. Victims include human rights defenders, dissidents, journalists, activists, and politicians.
- We provide a brief technical overview of the Candiru spyware's persistence mechanism and some details about the spyware's functionality.
- Candiru has made efforts to obscure its ownership structure, staffing, and investment partners. Nevertheless, we have been able to shed some light on those areas in this report.

## 1. Who is Candiru?

The company known as "Candiru," based in Tel Aviv, Israel, is a mercenary spyware firm that markets "untraceable" spyware to government customers. Their product offering includes solutions for spying on computers, mobile devices, and cloud accounts.

Figure 1: A distinctive mural of five men with empty heads wearing suits and bowler hats is displayed in this "Happy Hour" photo a previous Candiru office posted on Facebook by a catering company.[1]

### A Deliberately Opaque Corporate structure

Candiru makes efforts to keep its operations, infrastructure, and staff identities opaque to public scrutiny. Candiru Ltd. was founded in 2014 and has undergone several name changes[2] (*see: **Table 1***). Like many mercenary spyware corporations, the company reportedly recruits from the ranks of Unit 8200, the signals intelligence unit of the Israeli Defence Forces.

While the company's current name is Saito Tech Ltd, we will refer to them as "Candiru" as they are most well known by that name. The firm's corporate logo appears to be a silhouette of the reputedly-gruesome Candiru fish in the shape of the letter "C."

| Company name | Date of registration | Possible meaning |
|---|---|---|
| **Saito Tech Ltd.** (סאייטו טק בעיימ) | 2020 | "Saito" is a town in Japan |
| **Taveta Ltd.** (טאבטה בעיימ) | 2019 | "Taveta" is a town in Kenya |

| Company name | Date of registration | Possible meaning |
|---|---|---|
| **Grindavik Solutions Ltd.** (גרינדוויק פתרונות בעיימ) | 2018 | "Grindavik" is a town in Iceland |
| **DF Associates Ltd.** (ד. אפ אסוסיאייטס בעיימ) | 2017 | ? |
| **Candiru Ltd.** (קנדירו בעיימ) | 2014 | A parasitic freshwater fish |

**Table 1: Candiru's corporate registrations over time**

Candiru has at least one subsidiary: Sokoto Ltd.[3] *Section 5* provides further documentation of Candiru's corporate structure and ownership.

## Reported Sales and Investments

According to a lawsuit brought by a former employee, Candiru had sales of "nearly $30 million," within two years of its founding. The firm's reported clients are located in "Europe, the former Soviet Union, the Persian Gulf, Asia and Latin America." Additionally, reports of possible deals with several countries have been published:

- **Uzbekistan**: In a 2019 presentation at the Virus Bulletin security conference, a Kaspersky Lab researcher stated that Candiru likely sold its spyware to Uzbekistan's National Security Service.
- **Saudi Arabia & the UAE**: The same presentation also mentioned Saudi Arabia and the UAE as likely Candiru customers.
- **Singapore**: A 2019 *Intelligence Online* report mentions that Candiru was active in soliciting business from Singapore's intelligence services.
- **Qatar:** A 2020 *Intelligence Online* report notes that Candiru "has become closer to Qatar." A company linked to Qatar's sovereign wealth fund has invested in Candiru. No information on Qatar-based customers has yet emerged,

## Candiru's Spyware Offerings

A leaked Candiru project proposal published by TheMarker shows that Candiru's spyware can be installed using a number of different vectors, including malicious links, *man-in-the-middle* attacks, and physical attacks. A vector named "*Sherlock"* is also offered, that they claim works on Windows, iOS, and Android. This may be a browser-based zero-click vector.

**Infection Vectors**

| | |
|---|---|
| > Hyperlink | |
| > Weaponized file – Office file OR other (for Windows OS only) | **Included** |
| > Online physical attack vector (for Windows OS only) | |
| > Dissemination vector between platforms | |
| > Man in The Middle (MiTM) attack vector/price per browser | |
| > Sherlock for Windows, iOS and Android platforms – Optional | **(€6,000,000)** |
| > Integration to existing tactical solution | |

Figure 2: Infection vectors offered by Candiru.

Like many of its peers, Candiru appears to license its spyware by *number of concurrent infections*, which reflects the number of targets that can be under active surveillance at any one instant in time. Like NSO Group, Candiru also appears to restrict the customer to a set of approved countries.

The €16 million project proposal allows for an unlimited number of spyware infection attempts, but the monitoring of only 10 devices simultaneously. For an additional €1.5M, the customer can purchase the ability to monitor 15 additional devices simultaneously, and to infect devices in a single additional country. For an additional €5.5M, the customer can monitor 25 additional devices simultaneously, and conduct espionage in five more countries.

| | | |
|---|---|---|
| **Deployment Attempts** | | |
| Total number of agent deployment attempts | Unlimited | **Included** |
| **Agents Exfiltration Concurrency** | | |
| Total number of agents exfiltrating concurrently from all platforms | Up to 10 | **Included** |

SYSTEM ADDITIONAL PRICING OPTIONS

| NO. | ITEM DESCRIPTION | QTY. | TOTAL (EURO) |
|---|---|---|---|
| SYSTEM LICENSES | | | |
| 1 | **Additional 15 concurrent Infiltration Agents and 1 more country** (Total of X concurrent agents and XX countries) | 1 | **€1,500,000** |
| 2 | **Additional 25 concurrent Infiltration Agents and 5 more countries** (Total of X concurrent agents and XX countries) | 1 | **€5,500,000** |

Figure 3: Proposal for a Candiru Customer indicating number of concurrent infections under a given contract.
The fine print in the proposal states that the product will operate in "all agreed upon territories, "then mentions a list of restricted countries including the US, Russia, China, Israel and Iran. This same list of restricted countries has previously been mentioned by NSO Group. Nevertheless, Microsoft observed Candiru victims in Iran, suggesting that in some situations, products from Candiru do operate in restricted territories. In addition, targeting infrastructure disclosed in this report includes domains masquerading as the Russian postal service.

The proposal states that the spyware can exfiltrate private data from a number of apps and accounts including Gmail, Skype, Telegram, and Facebook. The spyware can also capture browsing history and passwords, turn on the target's webcam and microphone, and take pictures of the screen. Capturing data from additional apps, such as Signal Private Messenger, is sold as an add-on.

| | | |
|---|---|---|
| **Additional Agent Applications & Capabilities** | | |
| Retrieval of user cookies from supported browsers/price per browser | 1 | **€200,000** |
| Development and maintenance of the following applications: | | |
| • Twitter | 1 | **€200,000** |
| • Viber | 1 | **€200,000** |
| • Signal | 1 | **€500,000** |

Figure 4: Customers can pay additional money to capture data from Signal.
For a further additional €1.5M fee, customers can purchase a *remote shell* capability, which allows them full access to run any command or program on the target's computer. This kind of capability is especially concerning, given that it could also be used to download files, such as planting incriminating materials, *onto* an infected device.

## 2. Finding Candiru's Malware In The Wild

Using telemetry data from Team Cymru, along with assistance from civil society partners, the Citizen Lab was able to identify a computer that we suspected contained a persistent Candiru infection. We contacted the owner of the computer, a politically active individual in Western Europe, and arranged for the computer's hard drive to be imaged. We ultimately extracted a copy of Candiru's spyware from the disk image.

While analysis of the extracted spyware is ongoing, this section outlines initial findings about the spyware's persistence

### Persistence

Candiru's spyware was persistently installed on the computer via COM hijacking of the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32
```

Normally, this registry key's value points to the benign *Windows Management Instrumentation* wmiutils.dll file, but the value on the infected computer had been modified to point to a malicious DLL file that had been dropped inside the Windows system folder associated with the Japanese input method (IMEJP) C:\WINDOWS\system32\ime\IMEJP\IMJPUEXP.DLL. This folder is benign and included in a default install of Windows 10, but IMJPUEXP.DLL is not the name of a legitimate Windows component.

When Windows boots, it automatically loads the Windows Management Instrumentation service, which involves looking up the DLL path in the registry key, and then invoking the DLL.

## Loading the Spyware's Configuration

The IMJPUEXP DLL file has eight blobs in the PE resources section with identifiers 102, 103, 105, 106, 107, 108, 109, 110. The DLL decrypts these using an AES key and IV that are hardcoded in the DLL. Decryption is via Windows CryptoAPI, using AES-256-CBC.

Of particular note is resource 102, which contains the path to the legitimate wmiutils.dll, which is loaded after the spyware, ensuring that the COM hijack does not disrupt normal Windows functionality. Resource 103 points to a file AgentService.dat in a folder created by the spyware, C:\WINDOWS\system32\config\spp\Licenses\curv\config\tracing\. Resource 105 points to a second file in the same directory, KBDMAORI.dat.

IMJPUEXP.DLL decrypts and loads the AgentService.dat file whose path is in resource 103, using the same AES key and IV, and decompresses it via zlib. AgentService.dat file then loads the file in resource 105, KBDMAORI.dat, using a second AES key and IV hardcoded in AgentService.dat, and performs the decryption using a statically linked OpenSSL. Decrypting KBDMAORI.DAT yields a file with a series of nine encrypted blobs, each prefixed with an 8-byte little-endian length field. Each blob is encrypted with the same AES key and IV used to decrypt KBDMAORI.DAT, and is then zlib compressed.

The first four encrypted blobs appear to be DLLs from the Microsoft Visual C++ redistributable: vcruntime140.dll, msvcp140.dll, ucrtbase.dll, concrt140.dll. The subsequent blobs are part of the spyware, including components that are apparently called Internals.dll and Help.dll.  Both the Microsoft DLLs and the spyware DLLs in KBDMAORI.DAT are lightly obfuscated.  Reverting the following modifications makes the files valid DLLs:

1. The first two bytes of the file (MZ) have been zeroed.
2. The first 4 bytes of NT header (\x50\x45\x00\x00) have been zeroed.
3. The first 2 bytes of the optional header (\x0b\x02) have been zeroed.
4. The strings in the import directory have been XOR obfuscated, using a 48-byte XOR key hardcoded in AgentService.dat:
   `6604F922F90B65F2B10CE372555C0A0C0C5258B6842A83C7DC2EE4E58B363349F496E6B6A587A88D0164B74DAB9E6B58`

The final blob in KBDMAORI.DAT is the spyware's configuration in JSON format.  The configuration is somewhat obfuscated, but clearly contains Base64 UTF-16 encoded URLs for command-and-control.

```
"idecja+zq1T72cYcSXorfj2iqDE=": [
  "aAB0AHQAcABzADoALwAvAG0AcwBzAHQAbwByAGUALgBpAG8A",
  "aAB0AHQAcABzADoALwAvAGEAZAB0AHIAYQBjAGsAZQByAC4AbABpAG4AawA=",
  "aAB0AHQAcABzADoALwAvAGMAZABuAG0AbwBiAGkAbABlAC4AaQBvAA=="
],
```

Figure 5: The obfuscated spyware's C&C configuration in JSON format.
The C&C servers in the configuration are:

```
https://msstore[.]io
https://adtracker[.]link
https://cdnmobile[.]io
```

All three domain names pointed to 185.181.8[.]155. This IP address was connected to three other IPs that matched our Candiru fingerprint **CF1** (Section 3).

### Spyware Functionality

We are still reversing most of the spyware's functionality, but Candiru's Windows payload appears to include features for exfiltrating files, exporting all messages saved in the Windows version of the popular encrypted messaging app *Signal*, and stealing cookies and passwords from Chrome, Internet Explorer, Firefox, Safari, and Opera browsers. The spyware also makes use of a legitimate signed third-party driver, *physmem.sys*:

`c299063e3eae8ddc15839767e83b9808fd43418dc5a1af7e4f44b97ba53fbd3d`

Microsoft's analysis also established that the spyware could send messages from logged-in email and social media accounts directly on the victim's computer. This could allow malicious links or other messages to be sent *directly* from a compromised user's computer. Proving that the compromised user did not send the message could be quite challenging.

## 3. Mapping Candiru's Command & Control Infrastructure

To identify the websites used by Candiru's spyware, we developed four fingerprints and a new Internet scanning technique. We searched historical data from Censys and conducted our own scans in 2021. This led us to identify at least 764 domain names that we assess with moderate-high confidence to be used by Candiru and its customers. Examination of the domain names indicates a likely interest in targets in Asia, Europe, the Middle East, and North America.

Additionally, based on our analysis of Internet scanning data, we believe that there are Candiru systems operated from Saudi Arabia, Israel, UAE, Hungary, and Indonesia, among other countries.

### OPSEC Mistake by Candiru Leads to their Infrastructure

Using Censys, we found a self-signed TLS certificate that included the email address "amitn@candirusecurity.com". We attributed the candirusecurity[.]com domain name to Candiru Ltd, because a second domain name (*verification[.]center*) was registered in 2015 with a candirusecurity[.]com email address and a phone number (+972-54-2552428) listed by Dun & Bradstreet as the fax number for Candiru Ltd, also known as Saito Tech Ltd.

emailAddress=amitn@candirusecurity.com, C=US, ST=California, O=Internet Widgits Pty Ltd, emailAddress=amitn@candirusecurity.com

Certificate ▾ PEM Raw Data ▾ Explore ▾

**Basic Information**

| | |
|---|---|
| **Subject DN** | emailAddress=amitn@candirusecurity.com, C=US, ST=California, O=Internet Widgits Pty Ltd, emailAddress=amitn@candirusecurity.com |
| **Issuer DN** | emailAddress=amitn@candirusecurity.com, C=US, ST=California, O=Internet Widgits Pty Ltd, emailAddress=amitn@candirusecurity.com |
| **Serial** | Decimal: 15720440004717505221<br>Hex: 0xda2a38e4d206eac5 |
| **Validity** | 2016-05-15 13:05:07 **to** 2017-05-15 13:05:07 (365 days, 0:00:00) |

Figure 6: This Candiru certificate we found on Censys was the starting point of our analysis.
Censys data records that a total of six IP addresses returned this certificate: 151.236.23[.]93, 69.28.67[.]162, 176.123.26[.]67, 52.8.109[.]170, 5.135.115[.]40, 185.56.89[.]66. The latter four of these IP addresses subsequently returned another certificate, which we fingerprinted (**Fingerprint CF1**) based on distinctive features. We searched Censys data for this fingerprint.

```
SELECT parsed.fingerprint_sha256
FROM`censys-io.certificates_public.certificates`
WHERE parsed.issuer_dn IS NULL
 AND parsed.subject_dn IS NULL
 AND parsed.validity.length = 8639913600
 AND parsed.extensions.basic_constraints.is_ca
```

Table 2: Fingerprint CF1

We found 42 certificates on Censys matching **CF1**. We observed that six IPs matching **CF1** certificates later returned certificates that matched a second fingerprint we devised, **CF2**. The **CF2** fingerprint is based on certificates that match those generated by a “Fake Name” generator. We first ran an SQL query on Censys data for the fingerprint, and then filtered by a list of fake names.

```
SELECT parsed.fingerprint_sha256, parsed.subject_dn
FROM`censys-io.certificates_public.certificates`
WHERE (parsed.subject_dn = parsed.issuer_dn
   AND REGEXP_CONTAINS (parsed.subject_dn, r"^O=[A-Z][a-z]+,,?
   CN=[a-z]+\.(com|net|org)+$")
   AND parsed.extensions.basic_constraints.is_ca
```

Table 3: Fingerprint CF2 SQL Query.

The SQL query yielded 572 results. We filtered the results, requiring the TLS certificate’s organization in the parsed.subject_dn field to contain an entry from the list of 475 last names in the Perl Data-Faker module. We suspect that Candiru is using either this Perl module, or another module that uses the same word list, to generate fake names for TLS certificates. Neither the Perl Data-Faker module, nor other similar modules (e.g., the Ruby Faker Gem, or the PHP Faker module) appear to have built-in functionality for generating fake TLS certificates. Thus, we suspect that the TLS certificate generation code is custom code written by Candiru. After filtering, we found 542 matching certificates.

We then developed an HTTP fingerprint, called **BRIDGE**, with which we scanned the Internet and built a third TLS fingerprint, **CF3**. We are keeping the **BRIDGE** and **CF3** fingerprints confidential for now in order to maintain visibility into Candiru’s infrastructure.

## Overlap with CHAINSHOT

One of the IPs that matched our **CF1** fingerprint, 185.25.50[.]194, was pointed to by dl.nmcyclingexperience[.]com, which is mentioned as a final URL of a spyware payload delivered by the CHAINSHOT exploit kit in a 2018 report. CHAINSHOT is believed to be linked to Candiru, though no public reports have outlined the basis for this attribution, until now. Kaspersky has observed UAE hacking group *Stealth Falcon*[4] using CHAINSHOT, as well as an Uzbekistan-based customer that they call *SandCat*. While numerous analyses have focused on various CHAINSHOT exploitation techniques, we have not seen any public work that examines Candiru’s final Windows payload.

## Overlap with Google TAG Research

On 14 July 2021, Google’s Threat Analysis Group (TAG) published a report that mentions two Chrome zero-day exploits that TAG observed used against targets (**CVE-2021-21166** and **CVE-2021-30551**). The report mentions nine websites that Google determined were used to distribute the exploits. Eight of these websites pointed to IP addresses that matched our **CF3** Candiru fingerprint. We thus believe that the attacks that Google observed involving these Chrome exploits were linked to Candiru.

Google also linked a further Microsoft Office exploit they observed (**CVE-2021-33742**) to the same operator.

## Targeting Themes

Examination of Candiru’s targeting infrastructure permits us to make guesses about the location of potential targets, and topics and themes that Candiru operators believed that targets would find relevant and enticing.

Some of the themes strongly suggest that the targeting likely concerned civil society and political activity. This troubling indicator matches with Microsoft’s observation of the extensive targeting of members of civil society, academics, and the media with Candiru’s spyware. We observed evidence of targeting infrastructure masquerading as media, advocacy

organizations, international organizations, and others (s*ee: **Table 4***).

We found many aspects of this targeting concerning, such as the domain blacklivesmatters[.]info, which may be used to target individuals interested in or affiliated with this movement. Similarly, infrastructure masquerading as Amnesty International and Refugee International are troubling, as are lookalike domains for the United Nations, World Health Organization, and other international organizations. We also found the targeting theme of gender studies (e.g. womanstudies[.]co & genderconference[.]org) to be particularly interesting and warranting further investigation.

| Theme | Example Domains | Masquerading as |
|---|---|---|
| International Media | cnn24-7[.]online | CNN |
| dw-arabic[.]com | Deutsche Welle | |
| euro-news[.]online | Euronews | |
| rasef22[.]com | Raseef22 | |
| france-24[.]news | France 24 | |
| Advocacy Organizations | amnestyreports[.]com | Amnesty International |
| blacklivesmatters[.]info | Black Lives Matter movement | |
| refugeeinternational[.]org | Refugees International | |
| Gender Studies | womanstudies[.]co | Academic theme |
| genderconference[.]org | Academic conference | |
| Tech Companies | cortanaupdates[.]com | Microsoft |
| googlplay[.]store | Google | |
| apple-updates[.]online | Apple | |
| amazon-cz[.]eu | Amazon | |
| drpbx-update[.]net | Dropbox | |
| lenovo-setup[.]tk | Lenovo | |
| konferenciya-zoom[.]com | Zoom | |
| zcombinator[.]co | Y Combinator | |
| faceb00k-live[.]com | Facebook | |
| minstagram[.]net | Instagram | |
| twitt-live[.]com | Twitter | |
| youtubee[.]life | YouTube | |
| Popular Internet Websites | wikipediaathome[.]net | Wikipedia |
| International Organizations | osesgy-unmissions[.]org | Office of the Special Envoy of the Secretary-General for Yemen |
| un-asia[.]co | United Nations | |
| whoint[.]co | World Health Organization | |
| Government Contractors | vesteldefnce[.]io | Turkish defense contractor |

| Theme | Example Domains | Masquerading as |
|---|---|---|
| vfsglobal[.]fr | Visa services provider | |

**Table 4: Some targeting themes observed in Candiru domains.**

A range of targeting domains appears to be reasonably country-specific (s*ee: **Table 5***). We believe these domain themes indicate likely countries of *targets* and not necessarily the countries of the operators themselves.

| Country | Example Domain | What is this likely impersonating? |
|---|---|---|
| Indonesia | indoprogress[.]co | Left-leaning Indonesian publication |
| Russia | pochtarossiy[.]info | Russian postal service |
| Czechia | kupony-rohlik[.]cz | Czech grocery |
| Armenia | armenpress[.]net | State news agency of Armenia |
| Iran | tehrantimes[.]org | English-language daily newspaper in Iran |
| Turkey | yeni-safak[.]com | Turkish newspaper |
| Cyprus | cyprusnet[.]tk | A portal providing information on Cypriot businesses. |
| Austria | oiip[.]org | Austrian Institute for International Affairs |
| Palestine | lwaeh-iteham-alasra[.]com | Website that publishes Israeli court indictments of Palestinian prisoners |
| Saudi Arabia | mbsmetoo[.]com | Website for “an international campaign to support the case of Jamal Khashoggi” and other cases against Saudi Crown Prince Mohammed bin Salman |
| Slovenia | total-slovenia-news[.]net | English-language Slovenian news site. |

**Table 5: Some country themes observed in Candiru domains.**

## 4. A Saudi-Linked Cluster?

A document was uploaded from Iran to VirusTotal that used an *AutoOpen* Macro to launch a web browser, and navigated the browser to the URL https://cuturl[.]space/lty7uw, which VirusTotal recorded as redirecting to a URL, https://useproof[.]cc/1tUAE7A2Jn8WMmq/api, that mentions a domain we linked to Candiru, *useproof[.]cc*. The domain *useproof[.]cc* pointed to 109.70.236.107, which matched our fingerprint **CF3**.

The document was blank, except for a graphic containing the text “Minister of Foreign Affairs of the Islamic Republic of Iran.”

Figure 7: A document that loads a Candiru URL was uploaded to VirusTotal from Iran, and includes a header image referencing the Minister of Foreign Affairs.

We fingerprinted the behaviour of *cuturl[.]space* and traced it to five other URL shorteners: *llink[.]link*, *instagrarn[.]co*, *cuturl[.]app*, *url-tiny[.]co*, and *bitly[.]tel*. Interestingly, several of these domains were flagged by a researcher at ThreatConnect in two tweets, based on suspicious characteristics of their registration. We suspect that the AutoOpen format and the URL shorteners may be unique to a particular Candiru client.

A Saudi Twitter user contacted us and reported that Saudi users active on Twitter were receiving messages with suspicious short URLs, including links to the domain name *bitly[.]tel*. Given this, we suspect that the URL shorteners may be linked to Saudi Arabia.

## 5. Additional Corporate Details for Candiru

Ya'acov Weitzman (ויצמן יעקב) and Eran Shorer (שורר ערן) founded Candiru in 2014. Isaac Zack (זק יעקב), also reportedly an early investor in NSO Group, became the largest shareholder of Candiru less than two months after its founding and took a seat on its board of directors. In January 2019, Tomer Israeli (ישראלי תומר) first appeared in corporate records as Candiru's "director of finance," and Eitan Achlow (אחלאו איתן) was named CEO.

A number of independent investors appear to have funded Candiru's operations over the years. As of Candiru's notice of allotment of shares filed in February 2021 with the Israeli Corporations Authority, Zack, Shorer, and Weitzman are still the largest shareholders. Three organizations are the next largest shareholders: Universal Motors Israel LTD (corporate registration 511809071), ESOP management and trust services (איסופ שירותי ניהול) corporate registration 513699538, and Optas Industry Ltd. ESOP (corporate registration no. 513699538) is an Israeli company that provides employee stock program administrative services to corporate clients. We do not know whether ESOP holds its stock in trust for certain Candiru employees. Optas Industry Ltd. is a Malta-based private equity firm (registration number C91267, shareholder Leonard Joseph O'Brien, directors are O'Brien and Michael Ellul, incorporated 28 March 2019). It has been reported that for a decade O'Brien has served as head of investment and a board member of the Gulf Investment Fund, and that the sovereign Qatar Investment Authority has a 12% stake in the Gulf Investment Fund (through a subsidiary, Qatar Holding). Universal Motors Israel (company registration no. 511809071) as an investor (including a seat on Candiru's board) is curious considering their primary business is the distribution of new and used automobiles.

Besides Amit Ron (רון עמית), the Universal Motors Israel representative, Candiru's board as of December 2020 includes Isaac Zack, Ya'acov Weitzman, and Eran Shorer.

In addition to the involvement of Zack, Candiru shares other points of commonality with NSO Group, including representation by the same law firm and utilization of the same employee equity and trust administration services company.

## 6. Conclusion

Candiru's apparent widespread presence, and the use of its surveillance technology against global civil society, is a potent reminder that the mercenary spyware industry contains many players and is prone to widespread abuse. This case demonstrates, yet again, that in the absence of any international safeguards or strong government export controls, spyware vendors will sell to government clients who will routinely abuse their services. Many governments that are eager to acquire sophisticated surveillance technologies lack robust safeguards over their domestic and foreign security agencies. Many are characterized by poor human rights track records. It is not surprising that, in the absence of strong legal restraints, these types of government clients will misuse spyware services to track journalists, political opposition, human rights defenders, and other members of global civil society.

### Civil Society in the Crosshairs…*Again*

The apparent targeting of an individual because of their political beliefs and activities that are neither terrorist or criminal in nature is a troubling example of this dangerous situation. Microsoft's independent analysis is also disconcerting, discovering at least 100 victims of Candiru's malware operations that include "politicians, human rights activists, journalists, academics, embassy workers and political dissidents."

Equally disturbing in this regard is Candiru's registration of domains impersonating human rights NGOs (Amnesty International), legitimate social movements (Black Lives Matter), international health organizations (WHO), women's rights themes, and news organizations. Although we lack context around the specific use cases connected to these domains, their mere presence as part of Candiru's infrastructure—in light of widespread harms against civil society associated with the global spyware industry—is highly concerning and an area that merits further investigation.

### Rectifying Harms around the Commercial Spyware Market

Ultimately, tackling the malpractices of the spyware industry will require a robust, comprehensive approach that goes beyond efforts focused on a single high-profile company or country. Unfortunately, Israel's Ministry of Defense—from whom Israeli-based companies like Candiru must receive an export license before selling abroad—has so far proven itself unwilling to subject surveillance companies to the type of rigorous scrutiny that would be required to prevent abuses of the sort we and other organizations have identified. The export licensing process in that country is almost entirely opaque, lacking even the most basic measures of public accountability or transparency. It is our hope that reports such as this one will help spur policymakers and legislators in Israel and elsewhere to do more to prevent the mounting harms associated with an unregulated spyware marketplace.

It is worth noting the growing risks that spyware vendors and their ownership groups themselves face as a result of their own reckless sales. Mercenary spyware vendors like Candiru market their services to their government clients as "untraceable" tools that evade detection and thus prevent their clients' operations from being exposed. However, our research shows once again how specious these claims are. Although sometimes challenging, it is possible for researchers to detect and uncover targeted espionage using a variety of networking monitoring and other investigative techniques, as we have demonstrated in this report (and others like it). Even the most well-resourced surveillance companies make operational mistakes and leave digital traces, making their marketing claims about being stealthy and undetectable highly questionable. To the extent that their products are implicated in significant harms or cases of unlawful targeting, the negative exposure that comes from public interest research may create significant liabilities for ownership, shareholders, and others associated with these spyware companies.

Finally, this case shows the value of a community-wide approach to investigations into targeted espionage. In order to remedy the harms generated by this industry for innocent members of global civil society, cooperation among academic researchers, network defenders, threat intelligence teams, and technology platforms is critical. Our research drew upon multiple data sources curated by other groups and entities with whom we cooperated, and ultimately helped identify software vulnerabilities in a widely used product that were reported to and then patched by its vendor.

## Acknowledgements

Thanks to Microsoft and Microsoft Threat Intelligence Center (MSTIC) for their collaboration, and for working to quickly address the security issues identified through their research.

We are especially grateful to the targets that make the choice to work with us to help identify and expose the entities involved in targeting them. Without their participation this report would not have been possible.

Thanks to Team Cymru for providing access to their Pure Signal Recon product. Their tool's ability to show Internet traffic telemetry from the past three months provided the breakthrough we needed to identify the initial victim from Candiru's infrastructure

Funding for this project was provided by a generous grant from the John D. and Catherine T. MacArthur Foundation, the Ford Foundation, Oak Foundation, Sigrid Rausing Trust, and Open Societies Foundation.

Thanks to Miles Kenyon, Mari Zhou, and Adam Senft for communications, graphics, and organizational support.

1. 1. The same photo is visible in tweets by this reporter. ↩
2. 2. Data based on a review of the portfolio for company registration number 515126605 in the Israeli Corporations Authority online database. ↩
3. 3. Incorporated 14 Mar 2020, registration number 515996981, same registered address as Saito Tech. The name "Sokoto" may refer to a city in Nigeria. ↩
4. 4. Kaspersky calls this group *FruityArmor.* ↩