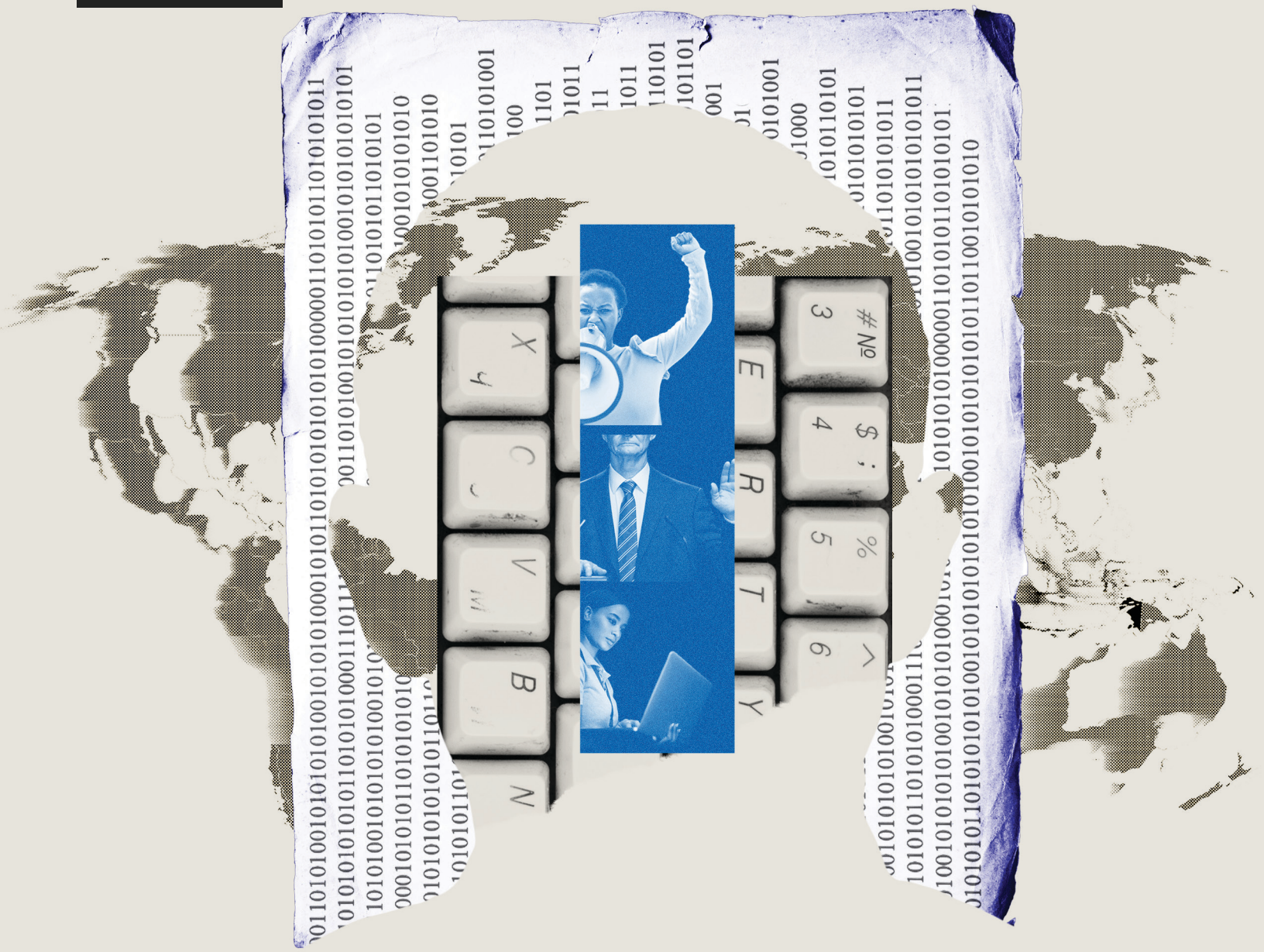
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 5, 2025



Tracking Candiru's DevilsTongue Spyware in Multiple Countries

Insikt Group identified new infrastructure tied to eight Candiru-linked clusters, including infrastructure for deploying and controlling DevilsTongue spyware and higher-tier operator infrastructure.

Using Recorded Future Network Intelligence, Insikt Group found that some clusters manage victim-facing infrastructure directly, while others use multiple layers or Tor to obscure operations.

Of the eight clusters found, five are likely active, including ones tied to Hungary and Saudi Arabia; one linked to Indonesia was active until November 2024, and two tied to Azerbaijan remain uncertain.

Note: The analysis cut-off date for this report was June 26, 2025

Executive Summary

Insikt Group identified new infrastructure associated with several clusters linked to the spyware vendor Candiru. This includes both victim-facing components likely used for deploying and controlling Candiru's DevilsTongue spyware, as well as higher-tier operator infrastructure. DevilsTongue is a sophisticated, modular Windows malware. The clusters vary in design and administration, with some directly managing victim-facing systems, while others use intermediaries or the Tor network. Eight distinct clusters were identified, with five being likely still active, including those linked to Hungary and Saudi Arabia. One cluster tied to Indonesia was active until November 2024, and two associated with Azerbaijan have uncertain status due to a lack of identified victim-facing infrastructure. Insikt Group also identified a company suspected to be part of Candiru's corporate network.

The use of mercenary spyware like DevilsTongue, both domestically and internationally, outside of serious crime or counterterrorism contexts, poses serious privacy, legal, and safety risks to targets, their organizations, and even the operators. Due to the high cost per deployment (based on researchers' assessments of leaked sales information), individuals with high intelligence value, such as politicians, business leaders, and individuals in sensitive roles, are often particularly at risk. Despite regulatory and legal efforts worldwide, including the US Department of Commerce adding Candiru to its Entity List, the EU's resolution to curb spyware abuse, and the UK- and France-led Pall Mall initiative to define and regulate legitimate use, Candiru has proven resilient, pushing back by trying to get removed from the entity list, for example, and continues to pose a significant threat.

In the short term, defenders should implement security best practices, including regular software updates, hunting for known indicators, pre-travel security briefings, and strict separation of personal and corporate devices. These measures should be supported by ongoing employee security awareness training to enhance understanding of infection vectors and malware capabilities and promote a culture of minimal data exposure. In the long term, organizations should invest in thorough risk assessments to inform more nuanced and adaptive security policies.

As the mercenary spyware market grows, with new vendors, products, and more countries seeking advanced cyber capabilities, the risk of being targeted now extends beyond civil society to anyone of interest to actors with access to such tools or their equivalents. At the same time, sustained profitability, rising competition, and stronger IT defenses are fueling innovation, as evidenced by alleged ad-based infections, direct attacks on messaging servers, and enhanced persistence (1, 2, 3). These trends are driving stealthier infection chains, targeting of cloud backups, a more professionalized spyware ecosystem, and broader tool portfolios. Effective mitigation, therefore, requires continuous ecosystem monitoring, thorough risk assessment, and stronger regulatory action from policymakers.

Key Findings

- Insikt Group has identified new infrastructure linked to several operational clusters associated with Candiru, an Israeli-based spyware vendor. This infrastructure includes both victim-facing components likely used in the deployment and C2 of Candiru's DevilsTongue spyware, and higher-tier infrastructure used by the spyware operators.
- Using Recorded Future Network Intelligence, Insikt Group identified significant differences in infrastructure design and administrative practices across the clusters. While some clusters manage their victim-facing infrastructure directly, others do so through intermediary infrastructure layers or via the Tor network.
- Eight distinct clusters were identified. Five are assessed as highly likely to be currently active, including ones associated with Hungary and Saudi Arabia. One cluster, highly likely linked to a customer based in Indonesia, was active until November 2024, while two others, associated with Azerbaijan, remain of uncertain status.

Background

Candiru, the Company

Candiru Ltd., now operating as Saito Tech Ltd., is an Israeli company that was founded in 2014 by Eran Shorer and Yaakov Weizmann. The company's original name, Candiru, draws from a notorious parasitic fish known for its stealth and invasiveness, a metaphor for the company's spyware capabilities. Isaac Zack, an early investor in NSO Group, was reported to be serving as Candiru's chairman. The company reportedly secured funding from the Founders Group, an angel syndicate co-founded by Omri Lavie and Shalev Hulio, the co-founders of NSO Group. Activity linked to the company is also tracked under the alias SOURGUM by Microsoft. In this report, Insikt Group uses the name Candiru, as this is the most widely known name for the company.

Over time, Candiru has frequently relocated its offices and restructured its corporate registration to maintain operational secrecy (see **Figure 1**).

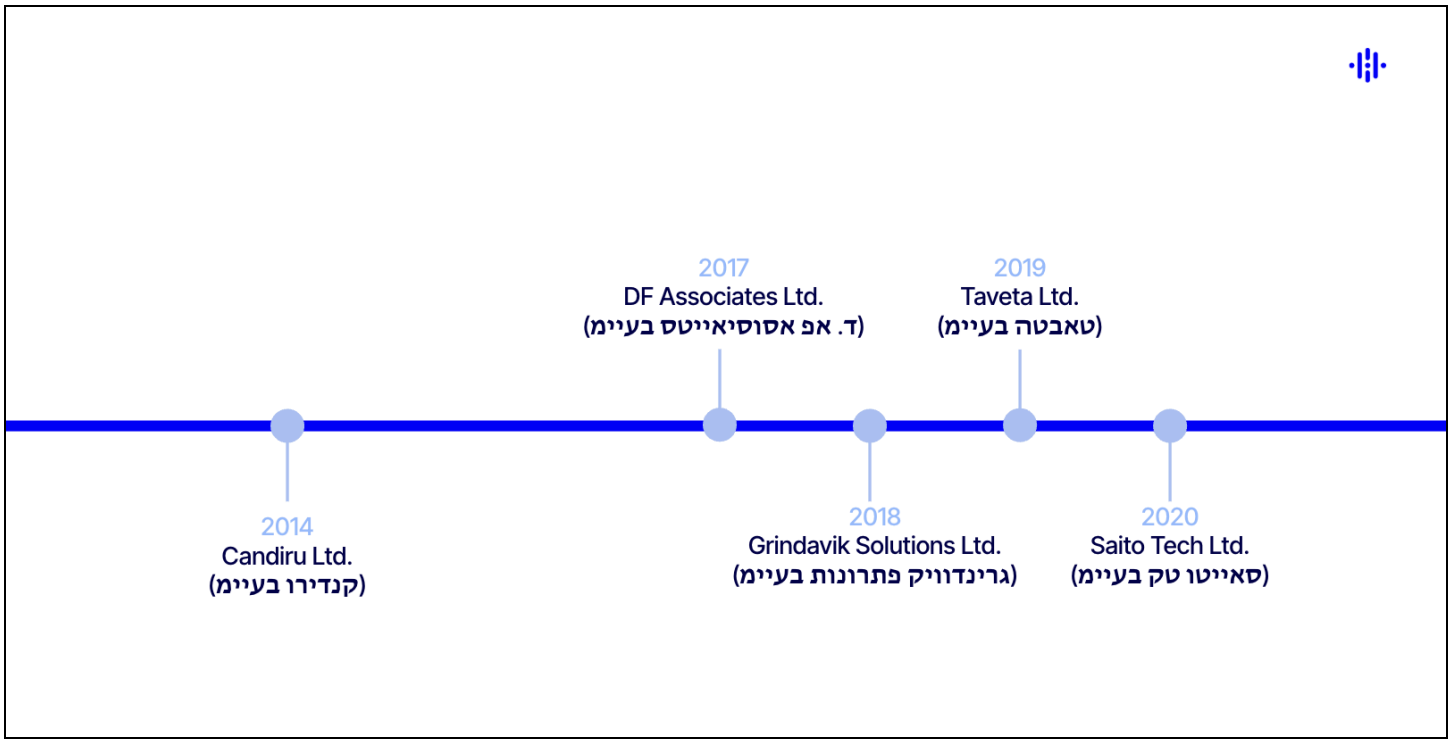


***Figure 1**: Timeline of Candiru's corporate registrations (Source: Recorded Future, derived from Citizen Lab)*

Court filings from a lawsuit brought by a former senior employee revealed that Candiru grew from 12 employees in 2015 to 70 by 2018. The company began securing contracts with government clients across Europe, the Middle East, Asia, and Latin America as early as 2016. That same year, it reportedly generated $10 million in revenue, which increased to $20–30 million by 2018, with an additional $367

million in pending deals involving 60 government clients. Negotiations were often conducted through local intermediaries.

In 2017, Candiru is believed to have started developing spyware for mobile devices, a development later confirmed by Israeli newspaper Haaretz, based on leaked internal documents. That same year, Candiru re-registered as DF Associates Ltd. (ד. אף אסוסיאייטס בעיימ).

In 2018, the company rebranded to Grindavik Solutions Ltd. (גרינדוויק פתרונות בעיימ).

By 2019, Candiru was valued at approximately $90 million, following the sale of a 10% equity stake by venture capitalist Eli Wartman to Universal Motors Israel (UMI). Reports also suggest investment from the Qatari sovereign wealth fund. That same year, Vice News reported that Kaspersky Lab had identified Candiru spyware in use by the Uzbekistan State Security Service (SSS). The SSS had reportedly used Kaspersky antivirus software to test the spyware's stealth and had configured an official government domain ("itt[.]uz") for its C2 communications. This leak led to the identification of other Candiru clients, including Saudi Arabia and the United Arab Emirates (UAE). The company renamed itself to Taveta Ltd. (טאבטה בעיימ) in 2019 as well.

In 2020, the company created a subsidiary named Sokoto. That same year, Candiru's board included founders Shorer and Weizmann, chairman Isaac Zack, and a representative from Universal Motors Israel. Candiru also changed its name to Saito Tech Ltd. (סאייטו טק בעיימ).

By 2021, company filings listed Universal Motors Israel, ESOP Management and Trust Services Ltd. (which manages employee stock ownership programs), and Optas Industry Ltd. (a proxy for the Qatari fund) as minority shareholders.

In April 2021, cybersecurity firm ESET uncovered an espionage operation using Candiru spyware in a watering hole attack targeting the UK news outlet Middle East Eye, news outlets associated with the Houthis and Hezbollah, and a likely dissident media outlet in Saudi Arabia. Additional victims included the websites of an Iranian embassy, Italian and South African aerospace firms, and Syrian and Yemeni government websites.

In July 2021, Citizen Lab and Microsoft revealed that Candiru's spyware had been widely deployed by multiple government clients, compromising at least 100 victims globally. The targets included politicians, human rights defenders, journalists, academics, embassy staff, and political dissidents. Microsoft reported that approximately half of the victims it observed were located in Palestine. The remaining victims were in Israel, Iran, Lebanon, Yemen, Spain (Catalonia), the United Kingdom, Türkiye, Armenia, and Singapore. The spyware's infrastructure was traced to several countries, including Saudi Arabia, Israel, the UAE, Hungary, and Indonesia. The domains used by Candiru also give a hint to the targets. Domains spoofed international media, advocacy organizations (including Black Lives Matter, Amnesty International, and Refugees International), gender studies events (including a conference on the topic), and international organizations (including the Office of the Special Envoy of the Secretary-General for Yemen, the UN, and the WHO).

In November 2021, the US Department of Commerce added both Candiru and NSO Group to its Entity List, citing their role in supplying spyware to foreign governments engaged in malicious activities.

In April 2022, Citizen Lab reported that members of the Catalan independence movement had been targeted with Candiru spyware as part of a domestic surveillance operation authorized by the Spanish government (see **Figure 2**). The campaign reportedly included surveillance of elected officials and political activists. Candiru specifically was used to target four Catalans working in the open-source and digital voting communities. One Catalan technologist, Elies Campo, was sent an email with a link that, if clicked, would have led to a Candiru infection while he resided in the US and had a US SIM card in his device. Additionally, Citizen Lab reported on the suspected targeting of Saudi Arabian social media users.

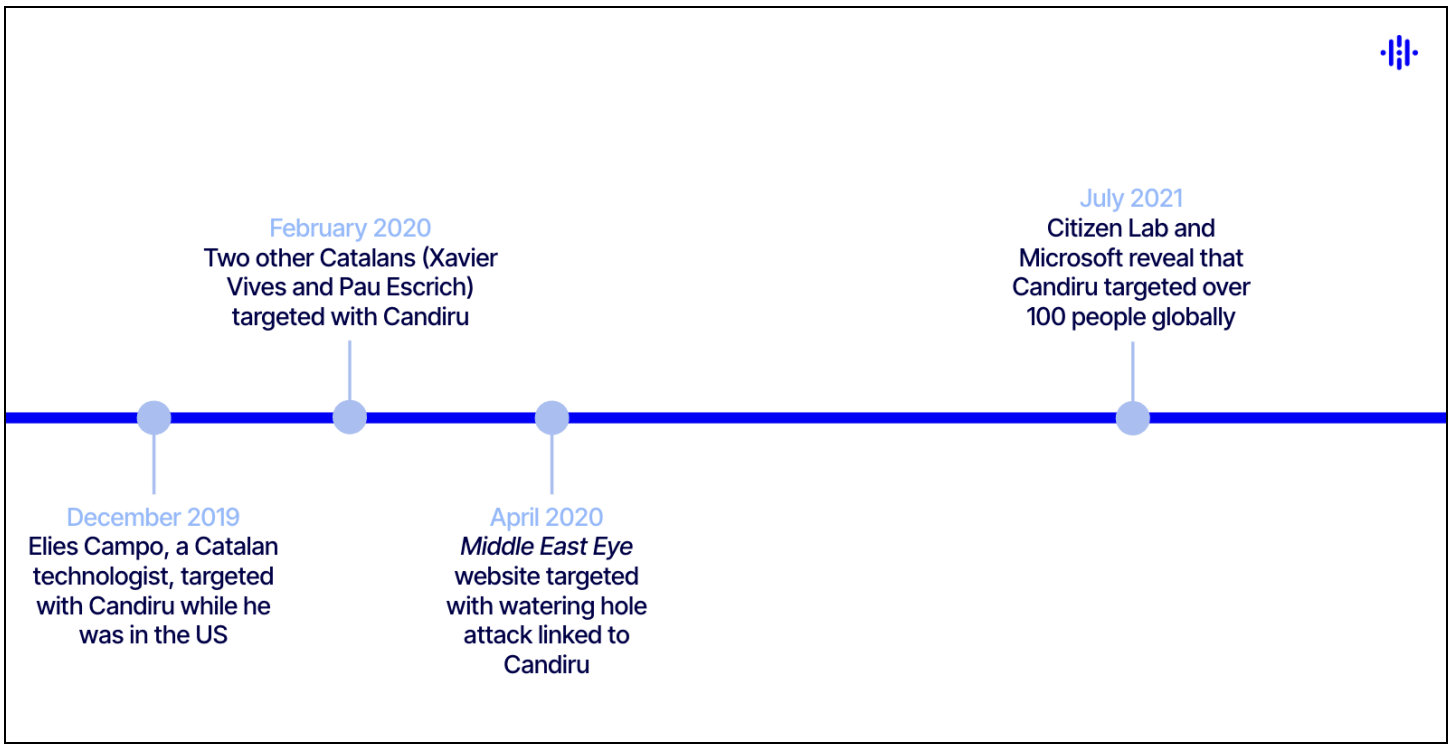


***Figure 2**: Timeline of Candiru targeting (Source: Recorded Future)*

Suspected New Company After Acquisition

In April 2025, the technology news outlet CTech reported that Candiru had been acquired several months earlier by Integrity Partners in a $30 million deal. Notably, Integrity Partners, an American investment firm whose partners include Elad Yoran (brother of Amit Yoran, former CEO of Tenable), had also previously placed a bid to acquire Pegasus spyware developer NSO Group.

The reporting indicates that Integrity Partners acquired Candiru's assets and transferred them, along with all company employees, to a newly established entity not currently subject to US government sanctions. By the time of the report, the first phase of the agreement had already been completed,

involving the transition of employees to the new entity for $10 million. The second phase, which entails the transfer of Candiru's export licenses, will be finalized once the necessary approvals are secured.

Notably, WHOIS records associated with Nerfwall, an alias linked to Candiru, led Insikt Group to identify the domain *integrity-labs[.]ltd*, registered on March 31, 2025. In this context, Insikt Group also identified a private Israeli company named Integrity Labs Ltd (אינטגריטי לאבס בע~מ), incorporated on December 18, 2024, under company number 517081089 and based in Herzliya, Israel. The company is directed by Naftali Yoran based on corporate report records attained by Recorded Future. Open-source reporting indicates that Elad Yoran is also known as Naftali Yoran.

Licensing Model

A leaked Candiru project proposal published by TheMarker, an Israeli news outlet, suggests that, similar to other spyware vendors like Intellexa, Candiru licenses its spyware according to the number of concurrent infections, which refers to the number of targets that can be actively monitored at any given moment. For example, one €16 million proposal allows for unlimited infection attempts but limits monitoring to ten devices simultaneously. Customers can expand this capacity: for an additional €1.5 million, they can monitor fifteen more devices and gain authorization to target one additional country; for €5.5 million, they can monitor 25 more devices and operate in five additional countries (see **Figure 3**). Another €1.5 million upgrade offers a remote shell capability, granting full command-line access to infected devices, raising particular concern due to its potential use for uploading files or planting incriminating content.

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**: Candiru pricing options (Source: Citizen Lab)*

The leaked proposal further states that the product is intended to operate solely within "agreed upon territories," explicitly listing the US, Russia, China, Israel, and Iran as restricted countries. Despite these limitations, Microsoft has identified Candiru victims in Iran and Israel, indicating that the spyware may, in certain cases, be deployed beyond its officially sanctioned regions. Corroborating this, the targeting infrastructure analyzed in Citizen Lab's report from 2021 includes domains impersonating the Russian postal service. That report also details the targeting of a Catalan technologist while he was living in the US, as mentioned above.

DevilsTongue

DevilsTongue, the name given by Microsoft to the Windows-based spyware developed by Candiru, is a complex, modular, multi-threaded malware written in C and C++ with a wide range of capabilities. Most of what is known about DevilsTongue stems from Microsoft's analysis and a leaked Candiru project proposal published by TheMarker. However, given the extensive list of suspected components and features, and the age of both reports, Insikt Group assesses that the malware's capabilities have likely evolved since then.

The leaked documents reveal that Candiru's spyware was designed for deep access to victim devices, enabling file extraction, browser data collection, and even the theft of encrypted messages from the Signal Messenger desktop app. **Figure 4** presents an excerpt from the leaked Candiru project proposal outlining the spyware's Windows-specific capabilities.

AGENT CAPABILITIES		
7	Skype	> Latest version + 6 months back > Social Media & Communication Applications
8	Outlook	
9	Telegram	
10	Facebook	> Social Media & Communication Applications
11	Gmail	
12	Device ID	> Device Information Applications
13	Browsing History	
14	Geolocation	
15	Network Map	
16	Files View	
17	Passwords	
18	Keylogger	> Hardware Applications
19	Webcam	
20	Microphone recording	
21	Screenshots	

***Figure 4**: Candiru's capabilities on Windows devices (Source: Citizen Lab)*

According to Microsoft's detailed analysis, DevilsTongue is a stealthy malware with both user- and kernel-mode components. It maintains persistence via COM hijacking by overwriting a legitimate COM class registry key's DLL path with a first-stage DLL dropped in `C:\Windows\system32\IME\`, and it stores encrypted second-stage payloads in the configuration directory. A signed third-party driver

(`physmem.sys`) enables kernel-level memory access and API call proxying to avoid detection. To preserve system stability, DevilsTongue reinjects the original COM DLL during hijacking, disguising this action through shellcode manipulation of the `LoadLibraryExW` return value. All additional payloads are decrypted and executed only in memory, allowing the malware to steal credentials from LSASS and browsers, access Signal messages, and use browser cookies to impersonate victims on platforms like Facebook, Gmail, and VK. The malware's use of scrubbed metadata, encryption, and unique hashes for each file further complicates detection and analysis.

Overlap with CHAINSHOT

CHAINSHOT is an exploit kit that has previously been associated with Candiru. It has been observed in use by threat actor groups such as Stealth Falcon and SandCat, the latter believed to be linked to the Uzbek government. SandCat drew significant attention in 2019 due to a series of operational security errors that not only exposed multiple zero-day vulnerabilities but also enabled direct attribution to Uzbekistan's State Security Service (SSS). Notably, another threat actor known as PuzzleMaker has also been mentioned in connection with CHAINSHOT, due to the use of a rare but likely not exclusively used technique. Although the connection between CHAINSHOT and Candiru was initially circumstantial, researchers at Citizen Lab later established a clearer link. They identified a shared fingerprint, including a matching IP address, that tied CHAINSHOT's final spyware delivery URL to infrastructure documented in a 2018 report by Palo Alto Networks, thereby reinforcing the association between CHAINSHOT and Candiru.

Initial Access Vectors

According to the leaked materials discussed above, Candiru's spyware can be deployed through multiple vectors, including malicious links, weaponized files, man-in-the-middle (MitM) attacks, and physical access. However, based on Insikt Group's current knowledge, public reporting has only confirmed the use of the first two vectors in documented cases involving Candiru-related infections, although it is highly likely that the other vectors have also been employed. When it comes to malicious links, Candiru has used both actor-controlled links, such as spearphishing emails and strategic website compromises known as watering hole attacks, to deliver its spyware, with infections typically involving exploits that target web browsers (1, 2).

For instance, Google's Threat Analysis Group (TAG) disclosed in 2021 that two Google Chrome renderer remote code execution zero-day vulnerabilities (CVE-2021-21166 and CVE-2021-30551) had been exploited by Candiru. These exploits were distributed via single-use links sent to specific targets, who were believed to be located in Armenia. The links directed recipients to attacker-controlled domains impersonating legitimate websites relevant to the victims' interests. Google TAG discovered that CVE-2021-21166 also affected WebKit, prompting Apple to patch it as CVE-2021-1844; however, there is no evidence it was used against Safari users.

In April 2021, Google TAG identified a campaign targeting Armenian users with malicious Office documents that loaded web content through Internet Explorer. This was achieved either by embedding

a remote ActiveX object using a `Shell.Explorer.1 OLE` object or by launching an Internet Explorer process via VBA macros to navigate to a web page. Following a fingerprinting phase, targets were served an Internet Explorer zero-day exploit, later assigned CVE-2021-33742 and patched by Microsoft in June 2021. TAG's analysis indicates that the Internet Explorer exploits were developed and supplied by the same entity responsible for the previously mentioned Google Chrome exploits.

In July 2022, Avast reported that CVE-2022-2294, a high-severity heap buffer overflow vulnerability in WebRTC within Google Chrome, was exploited to execute shellcode in the browser's renderer process, targeting users in the Middle East. The exploit, designed specifically for Windows, was likely combined with a sandbox escape, though the second-stage exploit could not be recovered. In Lebanon, the attackers compromised a website used by employees of a news agency, which contained signs of persistent cross-site scripting (XSS) attacks, likely as part of their testing phase, before ultimately injecting malicious JavaScript from an attacker-controlled domain. This injected code selectively redirected intended victims through a chain of attacker-controlled domains to the exploit server. Prior to Avast's report, ESET had reported on strategic web compromises across the Middle East, with a strong focus on Yemen, that they attributed to Candiru with medium confidence.

Beyond the previously mentioned vectors, reports from 2023 indicate that Candiru also possessed a capability known as Sherlock. Sherlock is a commercial surveillance capability developed by the Israeli software maker Insanet that is capable of infecting devices running Windows, Android, and iOS. Unlike traditional spyware that exploits software vulnerabilities, Sherlock leverages programmatic advertising to deliver its payload. By placing malicious ads through ad exchanges, it can target specific individuals based on demographics and location, leading to the covert installation of spyware when the ad is displayed on a user's device.

Threat Analysis

Over the past twelve months, Insikt Group has identified Candiru-related activity across eight distinct clusters, six of which are attributed to specific countries (see **Figure 5**). The observed activity spans both victim-facing infrastructure and higher-tier operational infrastructure. In at least one instance, Insikt Group linked higher-tier infrastructure associated with a specific cluster to infrastructure likely operated by Candiru itself.

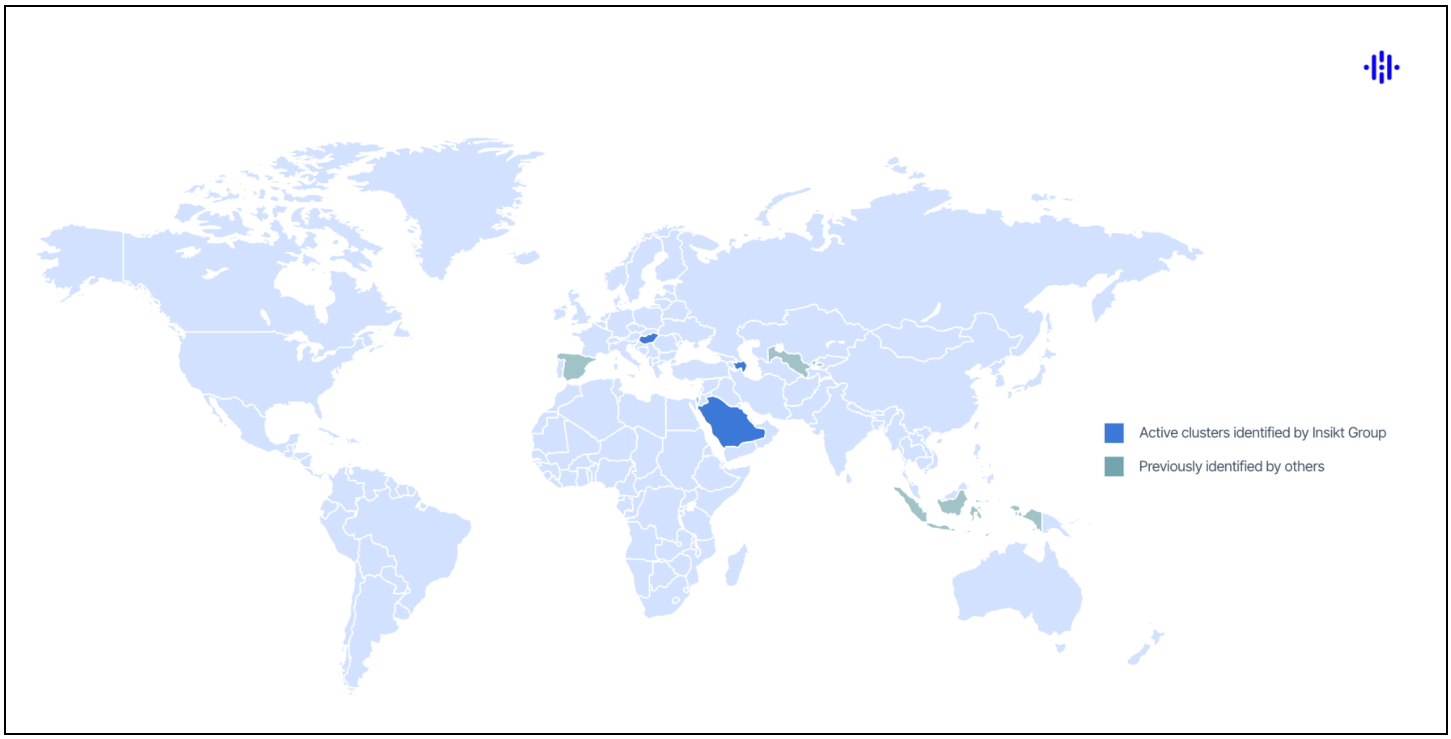


***Figure 5**: Countries with suspected customers of Candiru (Source: Recorded Future)*

Cluster 1: Hungary

Cluster 1, which is highly likely associated with a customer based in Hungary, has been active since at least 2019. The cluster manages its infrastructure through a combination of direct access, using a static internet service provider (ISP) IP address geolocated in the suspected customer country, and administration via a set of virtual private servers (VPSes) (see **Figure 6**). Although the reason for using both direct administration and an additional VPS layer remains unclear, it may reflect different operational procedures among customer operators.

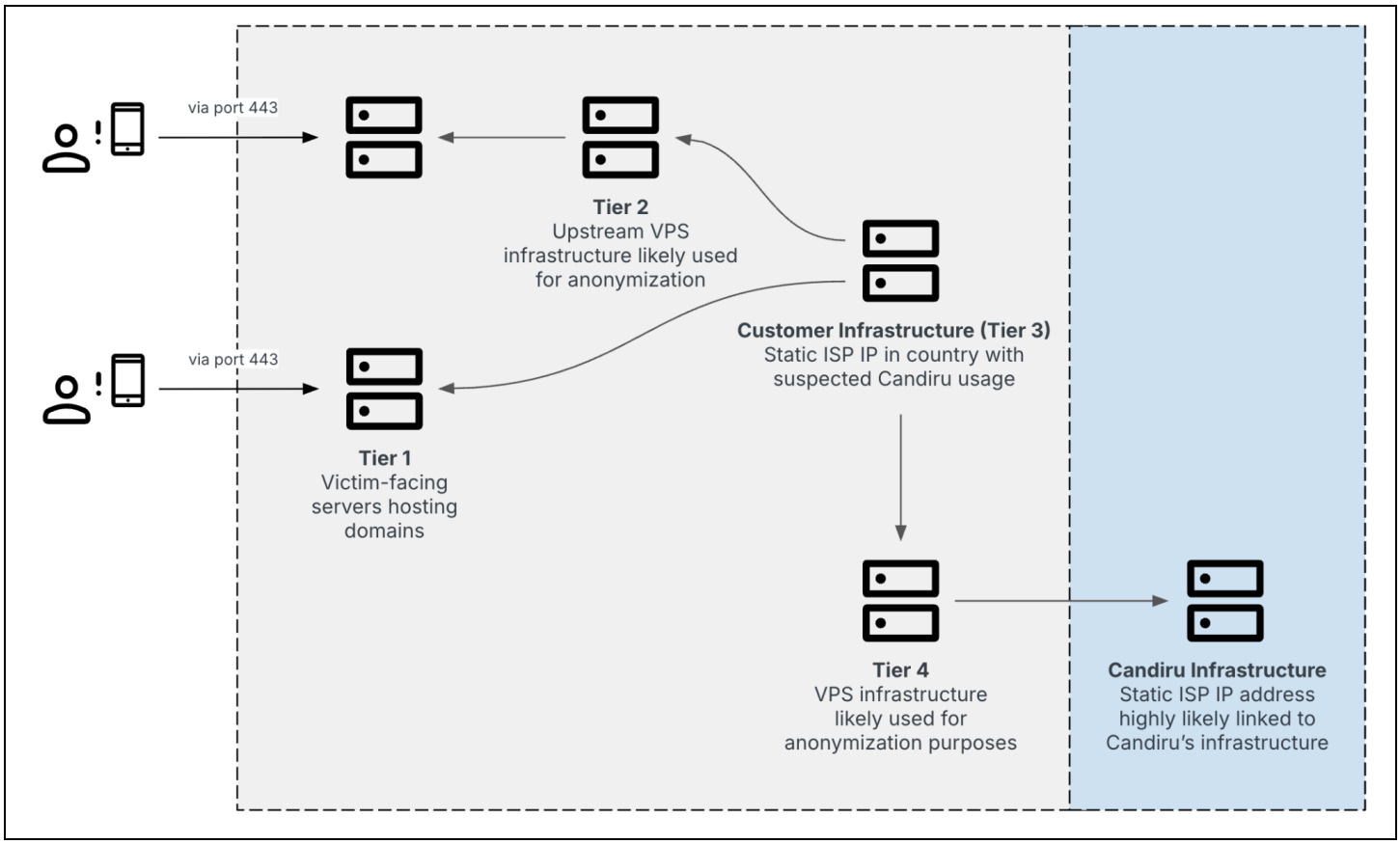


***Figure 6**: Network diagram of Cluster 1 (Source: Recorded Future)*

Of note, the static ISP IP address in use is associated with the same ASN previously observed in the deployment of another mercenary spyware product. Additionally, Insikt Group has observed the static ISP IP address communicating with infrastructure highly likely associated with Candiru via an intermediary hop. The precise purpose of this interaction is unknown, though it may be associated with licensing processes or software update routines.

Over the past twelve months, Insikt Group identified multiple victim-facing servers linked to Cluster 1 (see **Table 1**), many of which remain active at the time of writing. Although domains generally resolve to consistent IP addresses over time, at least one domain associated with Cluster 1 was observed changing its IP address. All identified IP addresses are announced by DigitalOcean.

Domain	IP Address	First Seen	Last Seen
ambiguouscommerce[.]com	134[.]209[.]3[.]89	2025-03-03	2025-06-23
bizarreclassify[.]com	165[.]22[.]5[.]231	2024-12-23	2025-06-13
conquerconfess[.]com	137[.]184[.]254[.]107	2024-12-28	2025-06-23
detaincharity[.]net	159[.]223[.]151[.]126	2024-12-26	2025-06-22
distractionfar[.]com	159[.]223[.]208[.]191	2025-05-21	2025-06-13
	161[.]35[.]150[.]79	2024-12-19	2025-05-13
exhibitexpanse[.]com	107[.]170[.]42[.]32	2025-03-03	2025-06-23
kartingrumble[.]com	159[.]89[.]14[.]225	2025-02-27	2025-06-17
sacrificeprincipal[.]net	134[.]209[.]220[.]157	2024-12-27	2025-06-22
salmonpride[.]net	147[.]182[.]161[.]167	2024-12-26	2025-06-23

***Table 1**: Domains and IP addresses linked to Cluster 1 (Source: Recorded Future)*

In 2021, Citizen Lab identified infrastructure artifacts suggesting that Hungary may have been a customer of Candiru. In mid-2024, Daniel Freund, a Member of the European Parliament (MEP) representing the Green Party and a critic of Hungarian Prime Minister Viktor Orbán, reported being the target of a phishing attack on May 27, 2024. The attack was suspected to involve Candiru spyware. Freund noted that, among the list of possible Candiru clients, Hungary appeared to be the "most likely" culprit. The phishing attempt involved an email purportedly sent by a student at Kyiv International University, inviting Freund to click on a link related to a seminar she claimed to be organizing.

Cluster 2: Saudi Arabia

Cluster 2, which is highly likely associated with a customer based in Saudi Arabia, has been active since at least 2020. The cluster manages its infrastructure through direct access, using a static ISP IP address geolocated in the suspected customer country (see **Figure 7**).

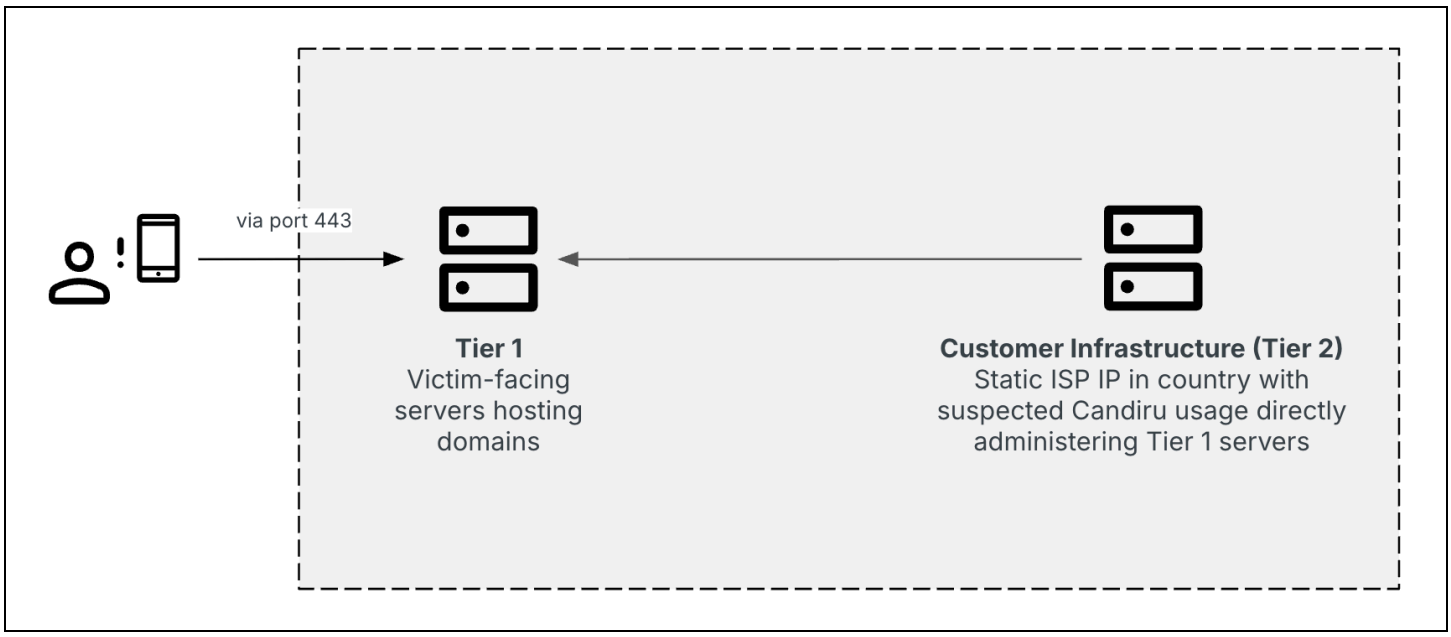


***Figure 7**: Network diagram of Cluster 2 (Source: Recorded Future)*

Over the past twelve months, Insikt Group identified a significant number of victim-facing servers linked to Cluster 2, many of which remain active at the time of writing (see **Table 2**). The identified IP addresses are announced by various ASes.

Domain	IP Address	First Seen	Last Seen
aperturebelt[.]com	146[.]70[.]29[.]228	2024-12-18	2025-06-23
asknapkin[.]com	84[.]247[.]51[.]183	2025-01-10	2025-06-23
beneathbreadth[.]com	146[.]70[.]102[.]134	2025-03-21	2025-06-22
breadgroomer[.]com	146[.]70[.]102[.]108	2024-12-10	2025-06-17
bypasscalculate[.]com	5[.]181[.]159[.]109	2025-03-25	2025-06-21
contradictionblindness[.]com	23[.]29[.]115[.]188	2024-08-27	2025-06-22
deardrill[.]com	146[.]70[.]20[.]203	2024-06-26	2025-06-09

Domain	IP Address	First Seen	Last Seen
foamdirection[.]com	188[.]208[.]141[.]190	2024-06-15	2025-05-30
groundbreakinginitative[.]com	23[.]227[.]198[.]196	2024-06-26	2025-06-03
hostilefauna[.]com	194[.]180[.]158[.]71	2025-03-27	2025-06-22
jellybat[.]net	146[.]70[.]53[.]156	2024-06-13	2025-05-18
leafconfuse[.]net	146[.]70[.]116[.]7	2025-01-08	2025-06-23
macromint[.]net	146[.]70[.]86[.]251	2025-01-22	2025-06-23
maturitygenesis[.]com	5[.]252[.]178[.]158	2025-01-08	2025-06-22
outdooutcome[.]com	194[.]180[.]191[.]84	2025-04-02	2025-06-19
patternperiod[.]com	146[.]70[.]169[.]165	2025-03-19	2025-06-22
pressaviation[.]com	146[.]70[.]147[.]9	2025-01-11	2025-06-22
signifyslight[.]com	194[.]37[.]97[.]159	2025-03-20	2025-06-21
stylebrakedown[.]com	146[.]70[.]102[.]121	2024-09-03	2025-06-22
suggestutterly[.]com	194[.]180[.]158[.]45	2025-03-25	2025-06-22
tidalscreen[.]com	146[.]70[.]81[.]218	2025-02-11	2025-06-15
tubeshape[.]com	91[.]207[.]173[.]115	2024-09-16	2025-06-20
windomination[.]com	146[.]70[.]160[.]49	2024-06-25	2025-06-04

***Table 2**: Domains and IP addresses linked to Cluster 2 (Source: Recorded Future)*

Citizen Lab reported on a potential Saudi Arabia-linked cluster in 2021 that likely targeted Iran and Saudi Arabian social media users using the "AutoOpen" Macro and URL shorteners.

Cluster 3: Unknown Attribution

Cluster 3 has not yet been attributed to any specific country. Based on insights from Recorded Future Network Intelligence, its victim-facing Tier 1 infrastructure appears to be operated via the Tor network. The infrastructure includes both suspected first- and second-stage servers, which are believed to be contacted sequentially during the infection process. **Table 3** shows the first-stage domains and IP addresses linked to Cluster 3, with the IP addresses all being linked to the hosting provider Vultr.

Domain	IP Address	First Seen	Last Seen
antperspective[.]com	208[.]85[.]18[.]104	2024-12-28	2025-06-26
baseagriculture[.]com	207[.]246[.]90[.]6	2024-12-12	2025-06-26
basicstraw[.]com	216[.]238[.]80[.]164	2024-12-30	2025-06-25
blockroster[.]net	65[.]20[.]96[.]9	2024-12-09	2025-06-25
bronzemonth[.]com	66[.]42[.]126[.]125	2025-03-06	2025-06-26
bypassbirch[.]com	149[.]28[.]77[.]207	2024-12-02	2025-06-23
bypasscommerce[.]com	95[.]179[.]215[.]54	2024-12-11	2025-06-25
cartoondrop[.]net	45[.]76[.]31[.]6	2024-11-03	2025-06-19
chickenstrawberry[.]com	45[.]32[.]109[.]170	2025-03-09	2025-06-26
closetmeat[.]com	140[.]82[.]5[.]20	2024-07-17	2025-06-25
commonclever[.]com	149[.]248[.]1[.]147	2024-12-13	2025-06-26
containsnow[.]com	149[.]28[.]142[.]211	2025-03-07	2025-06-25
convincechaotic[.]com	45[.]32[.]150[.]100	2025-03-03	2025-06-25
deliverconcern[.]net	207[.]246[.]105[.]206	2024-12-24	2025-06-17
deterdiffusion[.]com	149[.]28[.]71[.]25	2025-03-07	2025-06-21
drummerjourney[.]com	208[.]76[.]223[.]59	2025-02-25	2025-06-26
fearevolve[.]com[1]	45[.]77[.]105[.]76	2024-12-23	2025-06-26
isolatelecture[.]com	149[.]28[.]253[.]112	2025-03-10	2025-06-25
jobmarcher[.]com[2]	216[.]238[.]77[.]17	2024-12-09	2025-06-25
macrodrop[.]net	217[.]69[.]6[.]58	2024-12-27	2025-06-25
parkourbus[.]com	217[.]69[.]10[.]11	2025-03-07	2025-06-25
pepperdominate[.]com	70[.]34[.]194[.]5	2025-02-23	2025-06-26
prawnbasket[.]com	149[.]28[.]250[.]35	2025-03-06	2025-06-25

[1] Linked to DevilsTongue sample: 255869de85e2a171993fc5eb8a556d873a1b8966e040f6f55926f2fa2d595cc8
[2] Linked to DevilsTongue sample: 255869de85e2a171993fc5eb8a556d873a1b8966e040f6f55926f2fa2d595cc8

Domain	IP Address	First Seen	Last Seen
stablesurface[.]com	65[.]20[.]105[.]177	2024-11-11	2025-06-25
strangegarden[.]org	158[.]247[.]194[.]199	N/A	N/A

***Table 3**: Domains and IP addresses linked to Cluster 3 (Source: Recorded Future)*

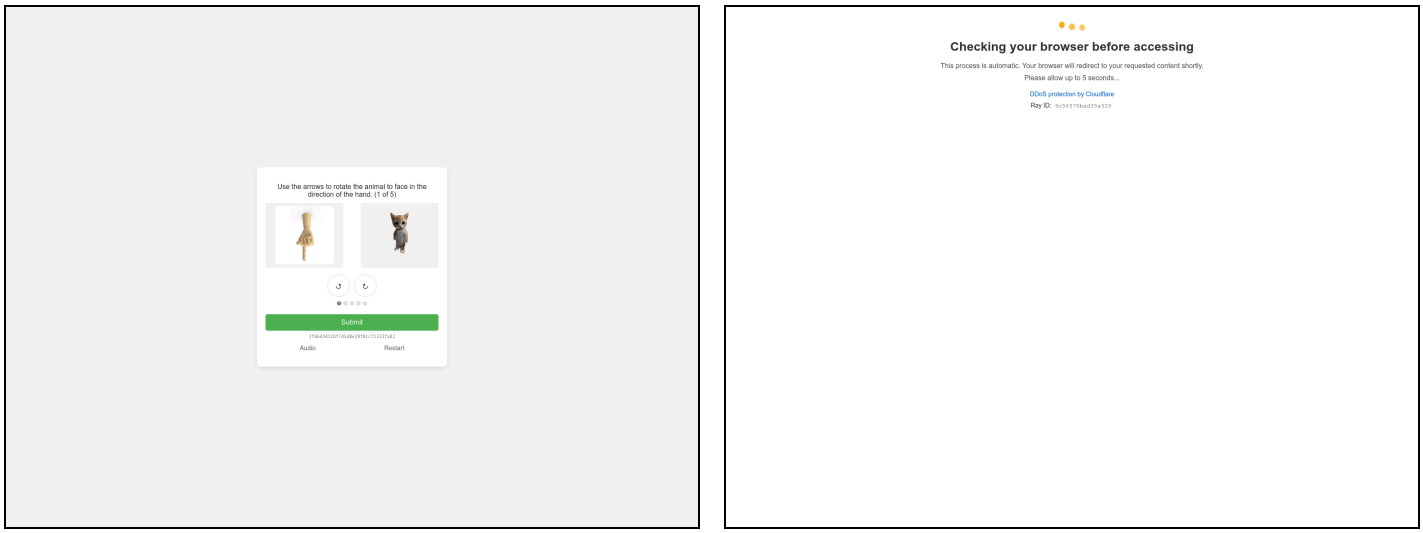
Additionally, Insikt Group identified suspected second-stage servers associated with Cluster 3, as detailed in **Table 4**. These second-stage IP addresses are announced by a wider range of ASes, including Vultr, DigitalOcean, and MVPS, among others.

Domain	IP Address	First Seen	Last Seen
bondmuscle[.]com	216[.]238[.]91[.]249	2025-01-29	2025-05-30
browniebell[.]com	164[.]92[.]225[.]66	2024-12-12	2025-06-18
calmbase[.]org	38[.]132[.]101[.]35	2025-05-07	2025-06-26
citecivilization[.]com	155[.]138[.]240[.]74	2024-12-18	2025-06-05
concretebottle[.]com	68[.]183[.]186[.]185	2025-03-07	2025-06-23
cottonbread[.]com	146[.]70[.]102[.]110	2024-12-11	2025-06-25
cranberrybear[.]com	139[.]59[.]14[.]26	2024-11-07	2025-06-24
damageconsider[.]com	66[.]42[.]73[.]169	2025-04-12	2025-06-24
dediccatedconsideration[.]com	167[.]99[.]85[.]48	2025-01-02	2025-06-21
dumplingbell[.]com	152[.]42[.]226[.]197	2025-01-06	2025-06-22
elifluousscintillam[.]com	165[.]22[.]51[.]81	2024-12-03	2025-06-18
eminententwine[.]com	198[.]211[.]98[.]248	2025-03-08	2025-06-12
fallaciousessential[.]net	104[.]207[.]153[.]0	2025-02-26	2025-06-20
finalsalami[.]com	208[.]76[.]221[.]167	2024-06-18	2025-05-25
goatsandals[.]com	165[.]22[.]71[.]71	2024-09-20	2025-06-26
guitarcalculate[.]com	185[.]234[.]52[.]230	2024-11-04	2025-06-25
journeyjest[.]net	64[.]225[.]3[.]138	2024-12-12	2025-06-25
notableexam[.]org	68[.]183[.]169[.]21	2025-05-30	2025-06-26

Domain	IP Address	First Seen	Last Seen
notionnowadays[.]com	45[.]77[.]57[.]173	2025-04-08	2025-05-22
penslice[.]com	70[.]34[.]251[.]208	2024-12-30	2025-06-20
predictproper[.]com	174[.]138[.]34[.]46	2024-12-01	2025-06-22
rollstrech[.]com	164[.]92[.]235[.]125	2024-11-02	2025-06-22
sunsetpotential[.]com	146[.]70[.]131[.]224	2024-11-15	2025-06-23
ultimatematter[.]info	167[.]99[.]3[.]150	2025-05-19	2025-06-25

***Table 4**: Domains and IP addresses linked to Cluster 3 (Source: Recorded Future)*

Notably, when scanned, some of the second-stage domains return identical, specific websites related to CAPTCHA and DDoS protection. (See **Figures 8** and **9**.) These exact websites have not been observed elsewhere, and while their purpose remains unclear, it is possible they are intended simply to blend in.



***Figures 8 and 9**: CAPTCHA and DDoS protection websites hosted on second-stage domains (Source: urlscan.io, urlscan.io)*

Additionally, Insikt Group identified a subdomain, likely associated with a free proxy service (see **Figure 10**), that resolved to the same IP address as the second-stage domain *dumplingbell[.]com*. Specifically, the subdomain *segawoncimengttd[.]yogifzvpnganteng[.]web[.]id* has been resolving to IP address *152[.]42[.]226[.]197* since December 17, 2024. This IP address began hosting *dumplingbell[.]com* on January 6, 2025. However, Insikt Group could not determine whether the IP address changed ownership during that period, or whether the subdomain's continued resolution to the IP address is incidental or connected to Candiru operations.

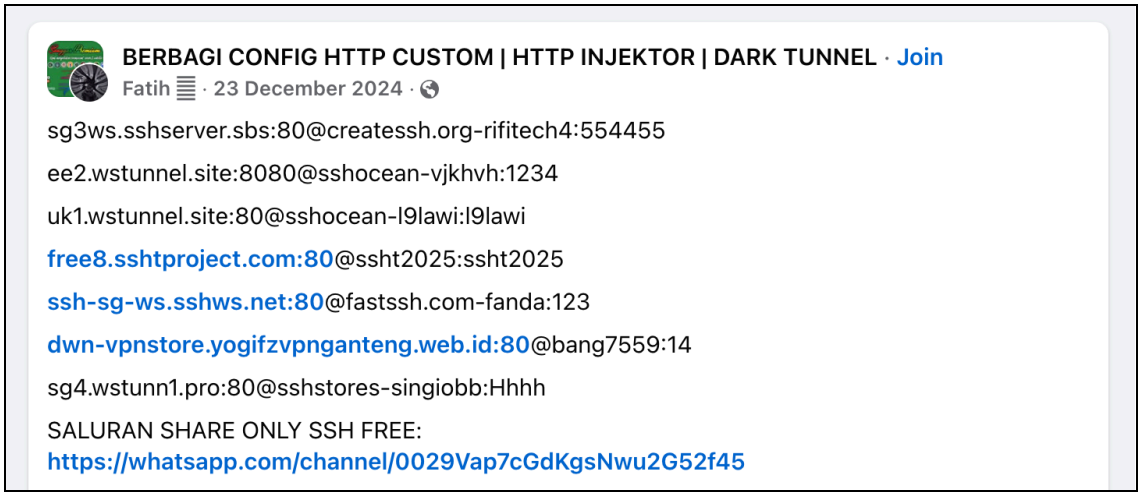


***Figure 10**: Facebook page offering various proxy-related services (Source: Recorded Future)*

Cluster 4: Unknown Attribution

Cluster 4 has not yet been attributed to any specific country. **Table 5** shows the domains and IP addresses linked to Cluster 4.

Domain	IP Address	First Seen	Last Seen
barnsecret[.]com	207[.]246[.]113[.]7	2024-05-29	2025-04-25
basinapposite[.]com	138[.]197[.]43[.]97	2024-12-26	2025-01-05
crossoverdue[.]com	149[.]28[.]57[.]173	2024-06-14	2025-06-13
desireeclipse[.]com	213[.]252[.]232[.]129	2025-01-23	2025-06-26
flexibleelevator[.]com	213[.]252[.]232[.]141	2025-01-22	2025-06-26
labyrinthextravagance[.]org	157[.]245[.]176[.]133	2025-04-09	2025-05-22
lessonhandle[.]com	65[.]20[.]106[.]49	2024-06-17	2025-05-31
parkourbus[.]com	217[.]69[.]10[.]11	2025-03-07	2025-06-25
profligatecensure[.]com	88[.]119[.]175[.]56	2025-01-05	2025-06-25
romancedrum[.]com	216[.]128[.]178[.]12	2024-06-18	2025-02-06
selectedpazzle[.]com	45[.]76[.]252[.]109	2024-06-16	2025-06-12
spongefruit[.]com	155[.]138[.]202[.]66	2024-06-13	2025-06-10
tacticscheap[.]net	88[.]119[.]175[.]75	2024-12-18	2025-06-25

***Table 5**: Domains and IP addresses linked to Cluster 4 (Source: Recorded Future)*

Notably, several IP addresses listed in **Table 5**, now associated with Cluster 4, were previously aligned with heuristics linked to Cluster 3 before shifting to patterns consistent with Cluster 4. Although the exact reason for this transition remains unverified, one plausible explanation is that changes in infrastructure deployments resulted in updated server configurations.

Cluster 5: Unknown Attribution

The cluster has not been attributed to any specific country but is assessed to have been active since at least 2023 (see **Table 6**). Insights from Recorded Future Network Intelligence indicate that it likely manages its victim-facing infrastructure directly, utilizing VPS hosts geolocated in Eastern Europe, as well as potentially leveraging the Tor network.

Domain	IP Address	First Seen	Last Seen
cooperatedisinfect[.]net	178[.]128[.]49[.]106	2025-04-08	2025-06-22
cropcritique[.]com	207[.]246[.]87[.]188	2024-12-13	2025-06-26
deducedefend[.]com	157[.]230[.]128[.]10	2024-12-17	2025-05-24
densefoot[.]com	136[.]244[.]69[.]219	2025-05-13	2025-06-26
devotionbelief[.]com	206[.]81[.]14[.]237	2024-08-16	2025-06-25
drivesplash[.]com	155[.]138[.]163[.]117	2024-08-29	2025-06-26
electric-prime[.]com	107[.]170[.]42[.]56	2024-10-10	2025-06-26
fileswaper[.]com	139[.]84[.]208[.]188	2024-11-20	2025-06-19
forecastgarden[.]com	64[.]226[.]103[.]163	2024-08-29	2025-06-23
golfconcert[.]com	199[.]247[.]10[.]38	2025-01-10	2025-06-18
measurecabin[.]com	149[.]28[.]242[.]133	2024-07-08	2025-06-25
mushroompalm[.]com	143[.]198[.]64[.]22	2025-01-09	2025-06-23
scoreparade[.]com	165[.]227[.]145[.]109	2024-11-14	2025-06-24
shareitwork[.]com	107[.]170[.]37[.]216	2024-11-11	2025-06-22
velvetpremier[.]com	216[.]238[.]86[.]164	2024-11-18	2025-06-24

***Table 6**: Domains and IP addresses linked to Cluster 5 (Source: Recorded Future)*

Other Clusters

In addition to the previously described clusters, Insikt Group has identified three more, with one assessed as likely inactive and two whose status remains unclear at the time of writing:

- The inactive cluster is likely associated with a customer based in Indonesia and appears to have remained active until November 2024. Indonesia has previously been linked to Candiru, as reported by Citizen Lab in 2021. This connection was further supported by Amnesty International in 2024, which analyzed shipment data related to cyber-surveillance systems delivered by the Singaporean firm Heha to the Indonesian National Police in 2020 and 2021. Their findings suggest that Candiru was likely the original supplier of the systems in question.
- Furthermore, the two clusters are highly likely tied to two customers in Azerbaijan. According to a 2024 investigation by the Israeli news outlet Haaretz, Azerbaijan was previously identified as a Candiru customer. However, Insikt Group has not observed any active victim-facing infrastructure linked to these clusters at the time of reporting, leaving their operational status uncertain.

Outlook

Insikt Group has uncovered new infrastructure linked to several operational clusters associated with Candiru, including both victim-facing components and higher-tier infrastructure used by the spyware operators. The identification of eight distinct clusters highlights Candiru's persistent global operations, which likely extend beyond known cases and continue despite public disclosures and US sanctions. However, several critical questions remain. Notably, Insikt Group identified that Candiru's assets may have been sold to an entity outside the scope of US sanctions, raising questions about the broader international impact on future sales. In addition, while some information has emerged about Candiru's initial access techniques, significant gaps in understanding remain, particularly regarding the technical mechanisms behind its alleged Sherlock infection vector, which has yet to be publicly documented from a technical perspective. Lastly, while reports indicate that Candiru has developed malware targeting operating systems beyond Windows, including spyware for mobile operating systems, there is currently no information available regarding its present status. Insikt Group will continue to monitor Candiru's activities and provide updates as new developments arise.

Appendix A — Indicators of Compromise (IoCs)

Domains:

ambiguouscommerce[.]com
antperspective[.]com
aperturebelt[.]com
asknapkin[.]com
barnsecret[.]com
baseagriculture[.]com
basicstraw[.]com
basinapposite[.]com
beneathbreadth[.]com
bizarreclassify[.]com
blockroster[.]net
bondmuscle[.]com
breadgroomer[.]com
bronzemonth[.]com
browniebell[.]com
bypassbirch[.]com
bypasscalculate[.]com
bypasscommerce[.]com
calmbase[.]org
cartoondrop[.]net
chickenstrawberry[.]com
citecivilization[.]com
closetmeat[.]com
commonclever[.]com
concretebottle[.]com
conquerconfess[.]com
containsnow[.]com
contradictionblindness[.]com
convincechaotic[.]com
cooperatedisinfect[.]net
cottonbread[.]com
cranberrybear[.]com
cropcritique[.]com
crossoverdue[.]com
damageconsider[.]com
deardrill[.]com
dediccatedconsideration[.]com
deducedefend[.]com
deliverconcern[.]net
densefoot[.]com
desireeclipse[.]com
detaincharity[.]net
deterdiffusion[.]com
devotionbelief[.]com
distractionfar[.]com
drivesplash[.]com
drummerjourney[.]com
dumplingbell[.]com

```
electric-prime[.]com
elifluousscintillam[.]com
eminententwine[.]com
exhibitexpanse[.]com
fallaciousessential[.]net
fearevolve[.]com
fileswaper[.]com
finalsalami[.]com
flexibleelevator[.]com
foamdirection[.]com
forecastgarden[.]com
goatsandals[.]com
golfconcert[.]com
groundbreakinginitative[.]com
guitarcalculate[.]com
hostilefauna[.]com
isolatelecture[.]com
jellybat[.]net
jobmarcher[.]com
journeyjest[.]net
kartingrumble[.]com
labyrinthextravagance[.]org
leafconfuse[.]net
lessonhandle[.]com
macrodrop[.]net
macromint[.]net
maturitygenesis[.]com
measurecabin[.]com
mushroompalm[.]com
notableexam[.]org
notionnowadays[.]com
outdooutcome[.]com
parkourbus[.]com
patternperiod[.]com
penslice[.]com
pepperdominate[.]com
prawnbasket[.]com
predictproper[.]com
pressaviation[.]com
profligatecensure[.]com
rollstrech[.]com
romancedrum[.]com
sacrificeprincipal[.]net
salmonpride[.]net
scoreparade[.]com
selectedpazzle[.]com
shareitwork[.]com
signifyslight[.]com
spongefruit[.]com
stablesurface[.]com
strangegarden[.]org
stylebrakedown[.]com
suggestutterly[.]com
```

sunsetpotential[.]com
tacticscheap[.]net
tidalscreen[.]com
tubeshape[.]com
ultimatematter[.]info
velvetpremier[.]com
windomination[.]com

IP Addresses:
23[.]227[.]198[.]196
23[.]29[.]115[.]188
38[.]132[.]101[.]35
45[.]32[.]109[.]170
45[.]32[.]150[.]100
45[.]76[.]252[.]109
45[.]76[.]31[.]6
45[.]77[.]105[.]76
45[.]77[.]57[.]173
5[.]181[.]159[.]109
5[.]252[.]178[.]158
64[.]225[.]3[.]138
64[.]226[.]103[.]163
65[.]20[.]105[.]177
65[.]20[.]106[.]49
65[.]20[.]96[.]9
66[.]42[.]126[.]125
66[.]42[.]73[.]169
68[.]183[.]169[.]21
68[.]183[.]186[.]185
70[.]34[.]194[.]5
70[.]34[.]251[.]208
84[.]247[.]51[.]183
88[.]119[.]175[.]56
88[.]119[.]175[.]75
91[.]207[.]173[.]115
95[.]179[.]215[.]54
104[.]207[.]153[.]0
107[.]170[.]37[.]216
107[.]170[.]42[.]32
107[.]170[.]42[.]56
134[.]209[.]220[.]157
134[.]209[.]3[.]89
136[.]244[.]69[.]219
137[.]184[.]254[.]107
138[.]197[.]43[.]97
139[.]59[.]14[.]26
139[.]84[.]208[.]188
140[.]82[.]5[.]20
143[.]198[.]64[.]22
146[.]70[.]102[.]108
146[.]70[.]102[.]110
146[.]70[.]102[.]121
146[.]70[.]102[.]134

146[.]70[.]116[.]7
146[.]70[.]131[.]224
146[.]70[.]147[.]9
146[.]70[.]160[.]49
146[.]70[.]169[.]165
146[.]70[.]20[.]203
146[.]70[.]29[.]228
146[.]70[.]53[.]156
146[.]70[.]81[.]218
146[.]70[.]86[.]251
147[.]182[.]161[.]167
149[.]248[.]1[.]147
149[.]28[.]142[.]211
149[.]28[.]242[.]133
149[.]28[.]250[.]35
149[.]28[.]253[.]112
149[.]28[.]57[.]173
149[.]28[.]71[.]25
149[.]28[.]77[.]207
152[.]42[.]226[.]197
155[.]138[.]163[.]117
155[.]138[.]202[.]66
155[.]138[.]240[.]74
157[.]230[.]128[.]10
157[.]245[.]176[.]133
158[.]247[.]194[.]199
159[.]223[.]151[.]126
159[.]223[.]208[.]191
159[.]89[.]14[.]225
161[.]35[.]150[.]79
164[.]92[.]225[.]66
164[.]92[.]235[.]125
165[.]227[.]145[.]109
165[.]22[.]51[.]81
165[.]22[.]5[.]231
165[.]22[.]71[.]71
167[.]99[.]3[.]150
167[.]99[.]85[.]48
174[.]138[.]34[.]46
178[.]128[.]49[.]106
185[.]234[.]52[.]230
188[.]208[.]141[.]190
194[.]180[.]158[.]45
194[.]180[.]158[.]71
194[.]180[.]191[.]84
194[.]37[.]97[.]159
198[.]211[.]98[.]248
199[.]247[.]10[.]38
206[.]81[.]14[.]237
207[.]246[.]105[.]206
207[.]246[.]87[.]188
207[.]246[.]90[.]6
207[.]246[.]113[.]7

208[.]76[.]221[.]167
208[.]76[.]223[.]59
208[.]85[.]18[.]104
213[.]252[.]232[.]129
213[.]252[.]232[.]141
216[.]128[.]178[.]12
216[.]238[.]77[.]17
216[.]238[.]80[.]164
216[.]238[.]86[.]164
216[.]238[.]91[.]249
217[.]69[.]10[.]11
217[.]69[.]10[.]11
217[.]69[.]6[.]58

DevilsTongue Hash (SHA256):
255869de85e2a171993fc5eb8a556d873a1b8966e040f6f55926f2fa2d595cc8

Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Initial Access: Spearphishing Link	T1566.002
Execution: Exploitation for Client Execution	T1203

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com