PREDATOR IN THE WIRES Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions

Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, Ron Deibert ⁝⁝ 9/22/2023

Apple has just issued an update for Apple products including iPhones, iPads, Mac computers, and Apple Watches. We encourage all users to immediately update their devices.

Key Findings

- Between May and September 2023, former Egyptian MP Ahmed Eltantawy was targeted with Cytrox's Predator spyware via links sent on SMS and WhatsApp. The targeting took place after Eltantawy publicly stated his plans to run for President in the 2024 Egyptian elections.
- In August and September 2023, Eltantawy's Vodafone Egypt mobile connection was persistently selected for targeting via network injection; when Eltantawy visited certain websites not using HTTPS, a device installed at the border of Vodafone Egypt's network automatically redirected him to a malicious website to infect his phone with Cytrox's Predator spyware.
- During our investigation, we worked with Google's Threat Analysis Group (TAG) to obtain an iPhone zero-day exploit chain (**CVE-2023-41991**, **CVE-2023-41992**, **CVE-2023-41993**) designed to install Predator on iOS versions through 16.6.1. We also obtained the first stage of the spyware, which has notable similarities to a sample of Cytrox's Predator spyware we obtained in 2021. We attribute the spyware to Cytrox's Predator spyware with high confidence.
- Given that Egypt is a known customer of Cytrox's Predator spyware, and the spyware was delivered via network injection from a device located physically inside Egypt, we attribute the network injection attack to the Egyptian government with high confidence.
- Eltantawy's phone was additionally infected with Cytrox's Predator spyware two years prior, in September [1] 2021, via a text message containing a link to a Predator website.

Background

Ahmed Eltantawy is a former Egyptian Member of Parliament who previously served as the chairman of Egypt's al-Karama political party. In March 2023 he announced his intention to run in the upcoming Egyptian presidential election, stating that he planned to offer a "democratic" alternative to the current president. Following this announcement Eltantawy, his family members, and supporters have been subjected to harassment, including reported arrests of 12 family members.

Egypt's current president Abdel Fattah el-Sisi has been in power since 2014, when he led the military overthrow of President Mohammed Morsi. Sisi has been widely described as an autocrat. Human rights groups, including Amnesty International and Human Rights Watch, have documented widespread human rights abuses under el-Sisi's regime, including repression against civil society groups, activists, and political opposition.

Eltantawy became suspicious about the safety of his phone and reached out to the Citizen Lab. We performed a forensic analysis on his device. Our forensic analysis showed numerous attempts to target Eltantawy with Cytrox's Predator spyware.

The Citizen Lab has previously documented Cytrox Predator infections targeting the devices of two exiled Egyptians: exiled politician Ayman Nour and the host of a popular news program (who chose to remain anonymous).

Zero-Day iOS Exploit Chain

While working with Eltantawy, the Citizen Lab and Google's Threats Analysis Group (TAG) obtained an iOS exploit chain that had been targeted at him. We initiated a responsible disclosure process with Apple, which assigned the following CVEs to vulnerabilities associated with the chain:

CVE-2023-41991 (Security): A malicious app may be able to bypass signature validation.
CVE-2023-41992 (Kernel): A local attacker may be able to elevate their privileges.
CVE-2023-41993 (WebKit): Processing web content may lead to arbitrary code execution.

On September 21, 2023, Apple released updates to multiple Apple products, which patches the vulnerabilities used by the exploit chain.

Click Here to read TAG's Blog Post.

Zero-day exploit chains for mobile devices can reportedly fetch into the millions of dollars from brokers that buy and sell these exploits.

Analysis of this chain is ongoing and we expect to publish a more extensive technical report in the future.

Fingerprinting and Scanning

The zero-day chain was hosted on sec-flare[.]com, and also contacted verifyurl[.]me. We fingerprinted these two websites (fingerprint **F1** for sec-flare[.]com and **F2** for verifyurl[.]me). We have identified a large number of IPs that matched our fingerprints, using Internet scanning. We consider all of these IPs (and the domain names returned in TLS certificates when they matched our fingerprints) to be linked to Cytrox's Predator spyware. While we investigate further, we are not releasing the domain names or IP addresses at this time.

Some of the domains we identified had names suggestive of tailoring towards specific countries or regions of focus include the Arabian Gulf, Southeast Asia, Angola, the Democratic Republic of the Congo, Egypt, Greece, Indonesia, Kazakhstan, Madagascar, Mongolia, the United Arab Emirates, and Sudan, which is a reported Cytrox customer. Of course, we cannot necessarily conclude that all of these governments are customers.

Attribution to Predator

The final stage of the iOS exploit chain was an iOS payload. We attribute the payload to Cytrox's Predator spyware with high confidence, based on comparing the payload with the 2021 sample of Predator we obtained. The two binaries share a key similarity, which we redact in order to preserve our visibility into future samples.

Additionally, some of the domain names we identified appeared to be geared at targets in countries previously identified as Cytrox Predator customers, including Egypt, Greece, and Madagascar.

Network Injection

In August and September 2023, when Eltantawy visited certain websites without HTTPS from his phone, using his Vodafone Egypt mobile data connection, he was silently redirected to a website (c.betly[.]me) via network injection. The domain betly[.]me matches our fingerprint **F1** for Cytrox's Predator spyware.

The injection was triggered based on the website specified in the HTTP *Host* header, as well as the value of the *User-Agent* header. The following reply was injected by an *on-path* middlebox, and the legitimate reply from the server was suppressed:

```
HTTP/1.1 307 Temporary Redirect
Via: 1.0 middlebox
Location: https://c.betly[.]me/[REDACTED]
Connection: close
```

The body of the destination website included two iframes, ID “if1” which contained apparently benign bait content (in this case a link to an APK file not containing spyware) and ID “if2” which was an invisible iframe containing a Predator infection link hosted on sec-flare[.]com.

Spyware Injection Localized to Egypt

We conducted a test to understand *where in the network* the injection happened. Ultimately, we were able to localize the injection to a link between Telecom Egypt and Vodafone Egypt. We cannot conclude from technical data alone whether the middlebox sits on the Telecom Egypt side or the Vodafone Egypt side of the link. However, we suspect that it is within Vodafone Egypt's network, because precisely targeting injection at an individual Vodafone subscriber would require integration with Vodafone's subscriber database.

Also, given that the injection is operating inside Egypt, the spyware is sold to government agencies, and Egypt is a known Predator customer, it is highly unlikely that this targeting occurred and that this setup was established outside of the purview of Egyptian authorities.

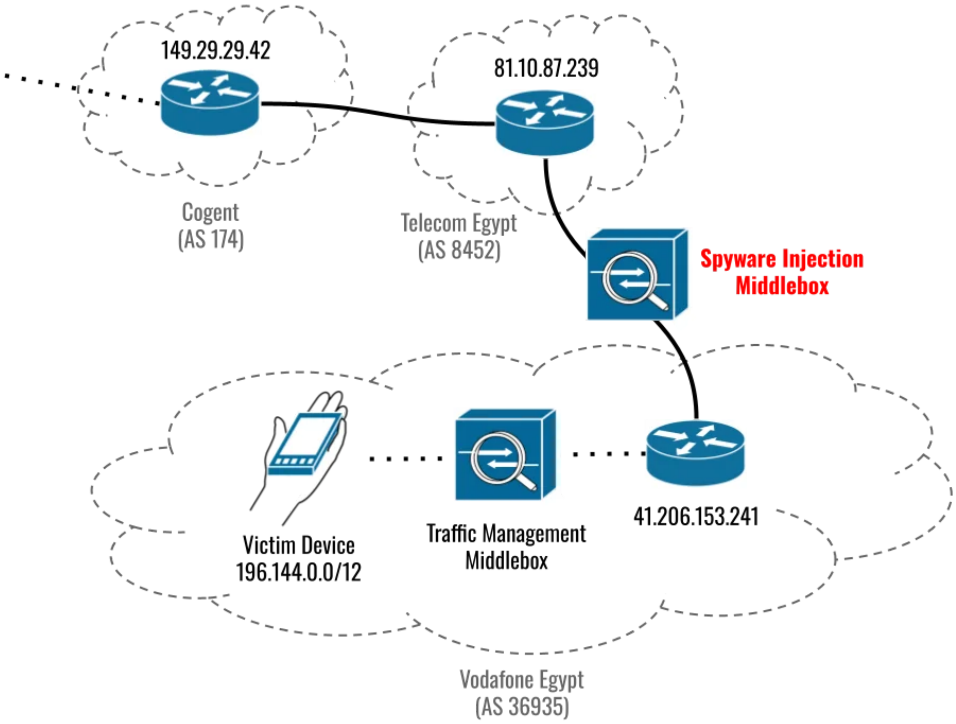


Figure 1: Network diagram showing the Spyware Injection Middlebox located on a link between Telecom Egypt and Vodafone

Process of Localizing the Spyware Injection

Typically, localizing the injection would involve sending packets from the targeted device (the "client") with increasing IP "Time To Live" (TTL) values. Since each router that handles a packet subtracts one from the IP TTL value, packets expire when TTL reaches zero, and routers typically identify their IP addresses to the packet's sender if they handle a sender's expired packet, we could locate the routers on either side of the injector. The routers on either side of the injector would be: (1) the router which reports an expired packet containing the highest TTL value for which the injector *does not* respond, and (2) the router which reports an expired packet containing the lowest TTL value for which the injector *does* respond. We could then identify which network the IP addresses belong to by looking them up in an IP WHOIS database.

Traditional Localization Technique Not Applicable

However, this technique was not applicable to Eltantawy's case because Vodafone Egypt's network appears to have a separate middlebox close to subscribers that manages all TCP connections. This middlebox, which we suspect is used for benign traffic management, is located at approximately IP TTL = 4 from Eltantawy. Since the traffic management middlebox rewrites packets with fixed TTL values, we cannot control the TTL value beyond the traffic management middlebox. We were however able to determine that the spyware injection was not located anywhere up to TTL = 4 from Eltantawy.

Injector Design Choices Enable Alternate Localization Technique

We identified two design choices in the injector, which, together, enabled us to localize the injection "in reverse", from a *measurement server* we controlled. First, the injector attempts to mask its presence by copying IP TTL values it receives into packets it injects. Second, when injecting a response to a client "from" a server, the injector takes the server's TTL to be the TTL from the *first* SYN/ACK it sees for a TCP connection, while ignoring TTL values in subsequent SYN/ACKs.

Together, these two design choices allow us to use our measurement server to "prime" the injector to inject a TTL = 1 packet to the client. To do this, our measurement server responds to a SYN by sending a SYN/ACK that reaches the injector with TTL = 1, and then sending a follow-up SYN/ACK with somewhat higher TTL such that it reaches the traffic management middlebox, completes the connection, and causes the traffic management middlebox to send the HTTP GET request that triggers the injection.

When the HTTP GET request reaches the injector, the injector sends a packet back to the client with TTL = 1. Because the injector is not directly adjacent to the client, the router immediately downstream from the injector will determine the packet is expired, and notify the sender of the injected packet. Because the injector spoofs the packet to come from our measurement server, the router identifies itself to us, notifying *our measurement server* of the packet's expiry. This process is illustrated in **Figure 2**.

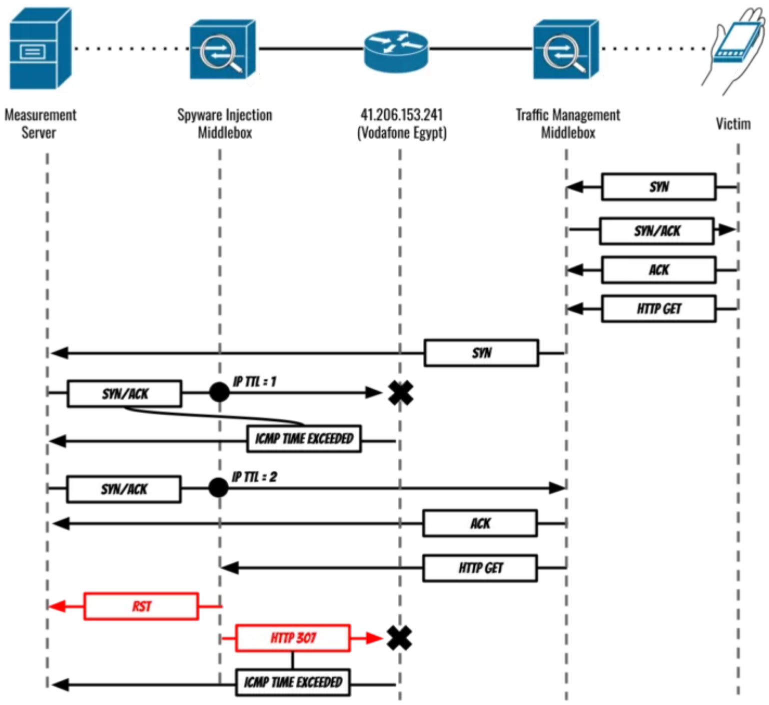


Figure 2: Diagram showing how we caused the Spyware Injection Middlebox to inject a packet containing an HTTP 307 redire an ICMP Time Exceeded message, allowing us to identify the next-hop downstream towards the victim from the Spyware Inje

Attributing the Injector

We attribute the spyware injection in Egypt to Sandvine's PacketLogic product with high confidence. Our attribution below has three parts.

First, we characterize the behavior of the spyware injection in Egypt. **Second**, we notice that the spyware injector in Egypt behaves entirely consistently with an injector used by Turk Telekom to implement a national sinkhole in Turkey. In a 2020 test, we noticed that the Turk Telekom injector matched our 2018 fingerprint for Sandvine PacketLogic devices. **Finally,** we observe that, while the Turk Telekom injector no longer matches our 2018 Sandvine PacketLogic fingerprint as of September 2023, it *still* contains a distinctive bug that we previously measured when it did match our 2018 Sandvine PacketLogic fingerprint.

Part One: Characterization of Spyware Injection in Egypt

Characterizing the spyware injection in Egypt was challenging, because of the presence of the Traffic Management Middlebox on Vodafone Egypt's network. This prevented us from seeing the raw packets sent by the spyware injector to Eltantawy's device.

Nevertheless, we were able to characterize the spyware injection in Egypt as follows:

1. The injected HTTP response to the client is a "307 Temporary Redirect" with the "Via: 1.0 middlebox" header set. At the same time, the injector sends a single TCP RST packet to the server.
2. If unacknowledged, the injector appears to re-send an identical packet up to four times (with a one second delay in between sends). If after five sends, the packet is not acknowledged, the injector sends a final terminating packet. Note that the traffic management middlebox does *not* transmit the raw packets; we observed these packets via ICMP Time Exceeded messages sent to us from 41.206.153.241. Unfortunately, due to size constraints in the payloads of ICMP error messages, the ICMP Time Exceeded messages did not quote the full packets that triggered them, though the included IP "total length" header value for the first five returned packets is an exact match for the "total length" header value of the 307 Temporary Redirect message redirect injected by the middlebox, and the IP "total length" header value for the last returned packet would be consistent with an empty TCP control packet, such as a TCP RST.
3. The injector appears to set TCP window size = 32120 in injected packets. Because of the traffic management middlebox, we cannot observe (from Eltantawy's side) the TCP window size values set in packets by the injector. Also, due to ICMP payload size constraints, the TCP window size value is not included in the ICMP Time Exceeded messages sent in response to the injected HTTP 307. However, we do observe TCP window size consistently set to 32120 in the RST injected to our measurement server.

Part Two: Egypt Spyware Injection Behavior Matches New Behavior from Devices in Turkey Previously Attributed to Sandvine

We noticed that the behavior was entirely consistent with the behavior of Turk Telekom's network injection capability, which we previously have attributed to Sandvine's PacketLogic devices. While Turk Telekom's network injection capability is used for a variety of purposes, the easiest to measure is Turkey's "national sinkhole", which redirects users who try to access websites on a list of "suspicious links" to a website run by Turkey's Computer Emergency Response Team (USOM). We measured this capability in December 2020, and found that the injection matched our 2018 fingerprint for Sandvine PacketLogic devices.

We conducted another measurement in September 2023, and found that the injection no longer matched our 2018 Sandvine PacketLogic fingerprint exactly, but was entirely consistent with the Egypt malware injection.

1. The injected HTTP response to the client is a "307 Temporary Redirect" with the "Via: 1.0 middlebox" header set. At the same time, the injector sends a single TCP RST packet to the server. **This is identical to the Egypt spyware injection.** The packet including the HTTP response has the FIN/ACK flags set. We could not determine the precise TCP flags set in the Egypt spyware case, due to ICMP payload size constraints, and the presence of the traffic management middlebox. However, FIN/ACK flags would be consistent with what we observed.
2. If unacknowledged, we observed the injector re-sending an identical redirect packet up to four times (with a one second delay in between sends). If after five sends, the packet is not acknowledged, the injector sends a final terminating packet. **This is identical to the Egypt spyware injection.** The final terminating packet is a TCP RST. We could not observe the precise TCP flags set in the Egypt spyware case, but an RST flag would be consistent with what we observed.
3. All injected packets have TCP window size set to 32120, regardless of TCP window values set by the client or server to the connection. This is consistent with the Egypt spyware injection.

Part Three: Devices in Turkey Previously Attributed to Sandvine Have Old Bug and Quirks Despite New Behavior

As of September 2023, the Turk Telekom injector *still matches* an odd bug we observed with their Sandvine PacketLogic deployment in December 2020, which leads us to conclude that Turk Telekom is still using Sandvine PacketLogic. Specifically, Turk Telekom's injector returns an injected (unencrypted) HTTP 307 Temporary Redirect message in response to a TLS Client Hello, which is an odd protocol violation.

Additionally, the Turk Telekom injector injects HTTP 307 Temporary Redirect messages in FIN/ACK packets, sets the TCP window size in all injected packets to 32120, and injects a single TCP RST packet to the server at the same time it injects the redirect to the client. All three of these are characteristics of our 2018 Sandvine PacketLogic fingerprint.

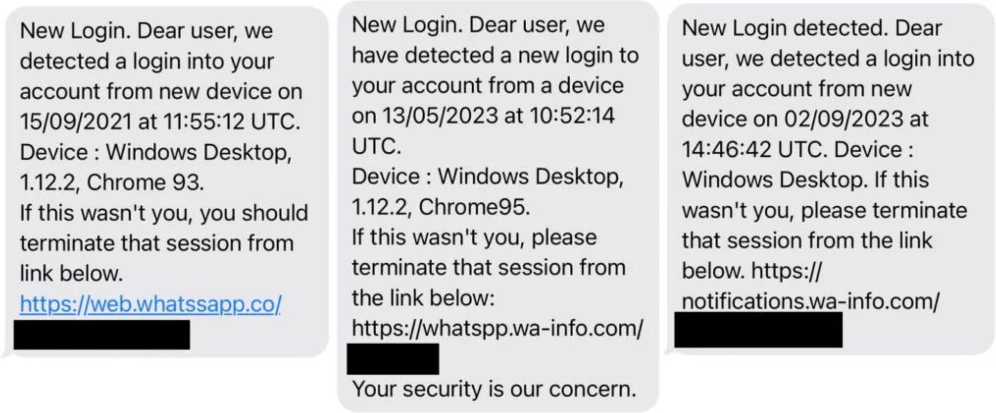
Conclusion: Egypt Spyware Injector is a Sandvine PacketLogic Product

Because the Turk Telecom injector still shows highly compelling similarities to its past behavior when we attributed it to Sandvine PacketLogic, and because the Turk Telecom injector's current behavior is fully consistent with the behavior of the Egypt spyware injector, we attribute the Egypt spyware injector to Sandvine PacketLogic with high confidence.

Targeting via SMS

Eltantawy additionally received several SMS messages in September 2021, May 2023, and September 2023 that posed as messages originating from WhatsApp.

The fraudulent messages invited Eltantawy to visit an included link to "terminate" what the messages said was a new login to Eltantawy's WhatsApp account. In reality, clicking the links would likely have infected Eltantawy's phone with Cytrox's Predator spyware.



New Login. Dear user, we detected a login into your account from new device on 15/09/2021 at 11:55:12 UTC.
Device : Windows Desktop, 1.12.2, Chrome 93.
If this wasn't you, you should terminate that session from link below.
https://web.whatssapp.co/
[redacted]

New Login. Dear user, we have detected a new login to your account from a device on 13/05/2023 at 10:52:14 UTC.
Device : Windows Desktop, 1.12.2, Chrome95.
If this wasn't you, please terminate that session from the link below:
https://whatspp.wa-info.com/
[redacted]
Your security is our concern.

New Login detected. Dear user, we detected a login into your account from new device on 02/09/2023 at 14:46:42 UTC. Device : Windows Desktop. If this wasn't you, please terminate that session from the link below. https://notifications.wa-info.com/
[redacted]

Figure 3: SMS messages sent to Eltantawy that we believe contained Predator infection links.

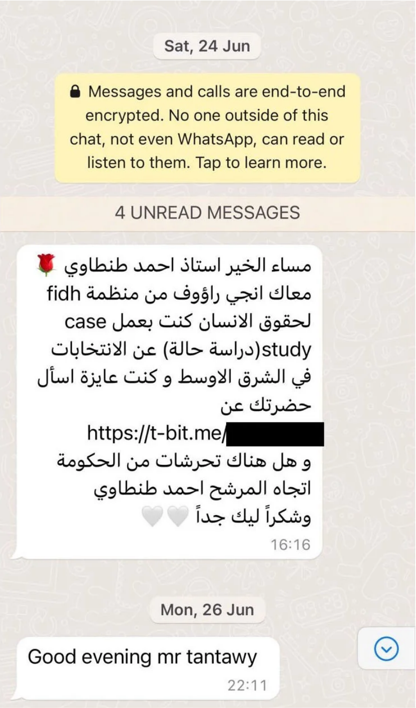
Interestingly, the domain names in the links do not match our **F1** or **F2** Predator fingerprint. However, approximately 2 minutes and 30 seconds after Eltantawy read the 15 September 2021 message, the Predator spyware was installed on his phone. We suspect that he clicked the message's link, triggering the installation. Since the 2023 messages contain similar bait content, we believe these messages were also attempts to install the Predator spyware on his phone.

We believe these websites are custom websites perhaps registered by a specific Predator customer. We believe that the following domain names are related:

```
almal-news[.]com
chat-support[.]support
cibeg[.]online
notifications-sec[.]com
wa-info[.]com
whatssapp[.]co
wts-app[.]info
```

WhatsApp Targeting

An individual purporting to be an "Angie Raouf" at the International Federation for Human Rights (FIDH) reached out to Eltantawy on WhatsApp, and sent him two Predator infection links to t-bit[.]me (matching fingerprint **F1**) on 24 June 2023 and 12 July 2023. The entire conversation was unread in Eltantawy's WhatsApp, indicating that he did not engage with these links.



Sat, 24 Jun

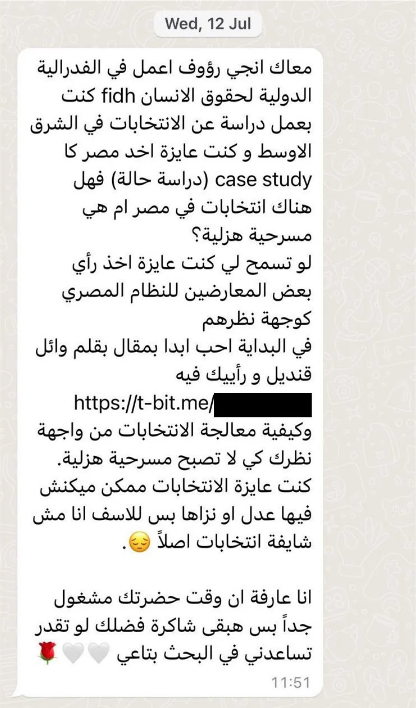
Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

4 UNREAD MESSAGES

مساء الخير استاذ احمد طنطاوي 🌹
معاك انجي راؤوف من منظمة fidh
لحقوق الانسان كنت بعمل case
study(دراسة حالة) عن الانتخابات
في الشرق الاوسط و كنت عايزة اسأل
حضرتك عن
https://t-bit.me/[redacted]
و هل هناك تحرشات من الحكومة
اتجاه المرشح احمد طنطاوي
وشكراً ليك جداً 🤍🤍
16:16

Mon, 26 Jun

Good evening mr tantawy
22:11



Wed, 12 Jul

معاك انجي رؤوف اعمل في الفدرالية
الدولية لحقوق الانسان fidh كنت
بعمل دراسة عن الانتخابات في الشرق
الاوسط و كنت عايزة اخد مصر كا
case study (دراسة حالة) فهل
هناك انتخابات في مصر ام هي
مسرحية هزلية؟
لو تسمح لي كنت عايزة اخذ رأي
بعض المعارضين للنظام المصري
كوجهة نظرهم
في البداية احب ابدا بمقال بقلم وائل
قنديل و رأييك فيه
https://t-bit.me/[redacted]
وكيفية معالجة الانتخابات من واجهة
نظرك كي لا تصبح مسرحية هزلية.
كنت عايزة الانتخابات ممكن ميكنش
فيها عدل او نزاها بس للاسف انا مش
شايفة انتخابات اصلاً 😔.

انا عارفة ان وقت حضرتك مشغول
جداً بس هبقى شاكرة فضلك لو تقدر
تساعدني في البحث بتاعي 🤍🤍🌹
11:51

We translate the messages in **Figure 4** below.

24 June	12 July
Good evening, Mr. Ahmed Tantawy This is Angie Raouf from FIDH organization for human rights. I was doing a case study on the elections in the middle east, and I wanted to ask you about [[LINK]] and whether there is harassment from the government towards the candidate Ahmed Tantawi. Thank you very much	This is Angie Raouf. I work at the International Federation for Human Rights FIDH, I was doing a study about elections in the Middle East, and wanted to take Egypt as a case study. Are there elections in Egypt, or is it just a comic play? If you allow me, I would like to get the opinion of those opposed to the Egyptian regime as their point of view. At the beginning, I would like to start with an article written by Wael Qandeel, and what do you think of it [[LINK]] How do you think elections should be done, so it won't become a comic play. I wanted elections even if it wasn't fair or just, but sadly I can't even see it as elections. I know that you are very busy, but I would be grateful if you could help me in my research.

Conclusion

The use of mercenary spyware to target a senior member of a country's democratic opposition after they had announced their intention to run for president is a clear interference in free and fair elections and violates the rights to freedom of expression, assembly, and privacy. It also directly contradicts how mercenary spyware firms publicly justify their sales.

President el-Sisi has been widely condemned for his autocratic rule, and Egypt's human rights abuses have been extensively documented. For any responsible company whose technology could be abused, the warning signs are clear. Yet, as evident in our report, insufficient due diligence was done to prevent these types of abuses by Cytrox or the other firms we have identified whose technology was employed to target and hack the device of Eltantawy.

This latest abuse case adds to the disturbing record of abuses connected to Cytrox and its Predator spyware. In addition to the other Egyptians whose devices were hacked with Predator spyware, we have also documented the hacking of Greek journalist Thanasis Koukasis with Predator spyware, and former Meta employee and dual Greek-American citizen, Artemis Seaford. Other investigations showed Predator spyware was used to hack the devices of a sitting member of the European Parliament, Nikos Androulakis, and was sold to notorious human rights abusers worldwide, including the genocidal militia in Sudan. For good reason, therefore, in July 2023 the US Commerce Department added Cytrox to the list of mercenary spyware firms on its designated entity list.

Our report also reveals the potential insecurities that run through the entire spectrum of the telecommunications ecosystem, including at the network layer, which can be exploited to inject malware on an unsuspecting users' device. Our internet communications are routed through many networks and middleboxes, some of which can be mis-used for malicious purposes, particularly if network requests flowing through them are not protected with cryptography. Although great strides have been made in recent years to "encrypt the web", users still occasionally visit websites without HTTPS, and a single non-HTTPS website visit can result in spyware infection. This report should serve as a reminder of the importance of achieving a 100% rate of HTTPS adoption.

Our report also concludes with high confidence that a Sandvine PacketLogic device was used to inject a redirect to malicious code in response to an internet request made by Eltantawy; the redirect subsequently delivered zero-day exploits in an attempt to infect his device with Cytrox's Predator spyware.

[2] This is not the first time we have identified the abuse of Sandvine's products; in 2018, the Citizen Lab documented the use of Sandvine's PacketLogic devices to inject malicious redirects into victims' web traffic in Turkey and redirect Egyptian Internet users to affiliate ads. Although that report was widely publicized, and we exchanged several letters with Sandvine and its legal representatives about the abuses we identified at the time, it appears that Sandvine's product is still being abused in Egypt. We have sent a letter to Sandvine notifying them of our findings and undertaking to publish any response we receive from them; as of the date of publication we have not yet received any reply.

This case also raises questions regarding a lack of sufficient controls around the export of technologies that can be used to violate human rights. This is not the first time that technology companies with Canadian headquarters are implicated in the export of technologies used in violation of international human rights law. While Canada has signed a recent Statement of Principles pledging to create and uphold domestic and international controls on commercial spyware technology, the Canadian government has not taken any concrete action around human rights and export controls with respect to dual-use technology.

In particular, we have recommended that the Canadian government ensure through law and meaningful sanctions that Canadian companies are prevented from exporting technologies to jurisdictions where there is a likelihood of human rights abuse. Significant steps must also be taken to ensure transparency into Canadian dual-use exports: there is no opportunity for public accountability without, at minimum, regular publication of detailed information regarding the type of dual-use items being exported, the name of the exporting company, and the identity of the end-user. Further, Canadian companies should also be subject to human rights due diligence obligations that are enforced through law and appropriate penalties.

Update Apple Devices Now & Enable Lockdown Mode

We urge everyone to immediately update their devices.

Patched versions are: macOS Ventura 13.6, macOS Monterey 12.7, watchOS 9.6.3, watchOS 10.0.1, iOS 16.7 and iPadOS 16.7, iOS 17.0.1 and iPadOS 17.0.1.

As with the BLASTPASS zero-click exploit we recently disclosed, we believe, and Apple's Security Engineering and Architecture team has confirmed to us, that Lockdown Mode blocks this particular attack.

These two recent high profile cases underline the serious value that this security mode provides.

Therefore, **we encourage all Mac, iPhone, and iPad users who may face increased risk because of who they are or what they do to enable Lockdown Mode.**

Acknowledgments

Special thanks to Ahmed Eltantawy who chose to assist us in investigating his case. We would like to acknowledge his bravery in coming forward publicly. Without his collaboration, the discovery of these CVEs would not have been possible.

Special thanks to Jakub Dalek, Jeff Knockel, and Adam Senft for assistance and review.

Thanks to the entire team at Google TAG, especially Maddie Stone, for their collaboration in this investigation.

Thanks to multiple teams at Apple for their rapid response and patch cycle.

We'd also like to thank TNG.

1. Typo corrected on September 25, 2023.
   ↩

- This sentence was edited for clarity on September 25, 2023.

↩