Independently Confirming Amnesty Security Lab's finding of Predator targeting of U.S. & other elected officials on Twitter/X - The Citizen Lab

Archived: 2026-04-06 00:12:54 UTC

Amnesty International's Security Lab has just published *Caught in the Net* as part of the European Investigative Collaborations' *Predator Files*, which details a threat actor sending what they assess to be Predator infection links on social media in replies to Twitter / X posts by officials, journalists and other members of civil society.

The Citizen Lab independently received and collected a set of since-deleted posts by this threat actor, which we call ***REPLYSPY***. Our findings align with the Security Lab's conclusions concerning Cytrox infrastructure, and we assess with high confidence that ***REPLYSPY*** included Cytrox Predator infection links in replies to numerous U.S. and international officials and others.

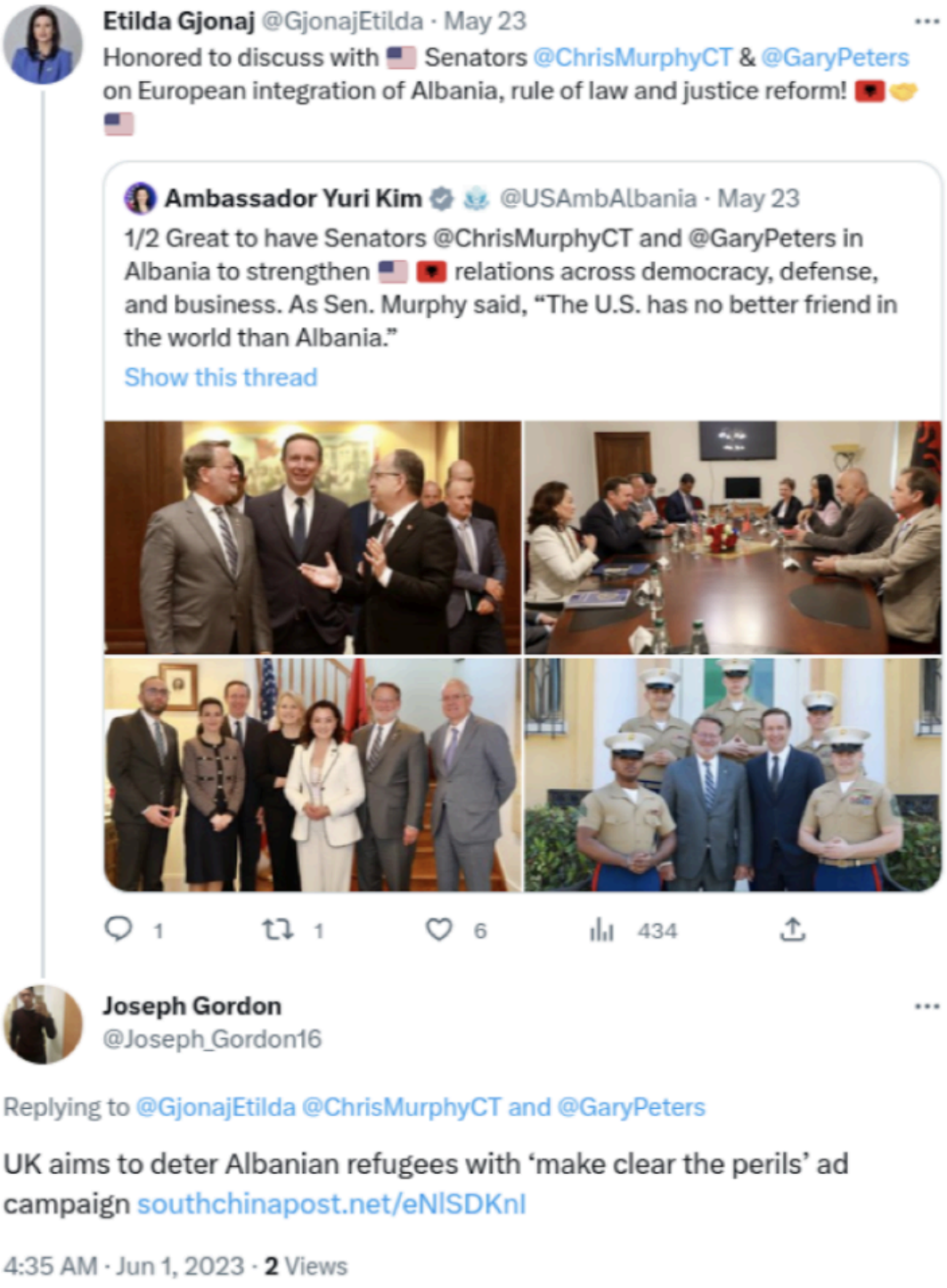
If a user clicked on one of the links, and a validation procedure (see: **Section 2**) was satisfied, the user's device would have been infected with Cytrox's Predator spyware, likely using a chain of zero-day exploits. Cytrox is a subsidiary of surveillance conglomerate Intellexa.

This note briefly describes some aspects of the observed targeting, as well as elements of Predator's installation validation process that Citizen Lab has observed in 2023.

1. US & foreign elected officials: mercenary spyware targets

On May 23, 2023, Albanian politician Etilda Gjonaj quote-tweeted a tweet by US Ambassador to Albania Yuri Kim that mentioned Senator Chris Murphy and Senator Gary Peters. Senator Murphy was tagged on his official account, while Senator Peters was tagged on his campaign account.

On June 1, 2023, the primary ***REPLYSPY*** account "Joseph Gordon" (@Joseph_Gordon16) responded to this tweet with another tweet containing a link, as well as the text "UK aims to deter Albanian refugees with 'make clear the perils' ad campaign", the headline of a recent article published by Hong Kong English-language newspaper South China Morning Post. However, the link included by Gordon was not a link to the official website of the South China Morning Post (*scmp.com*) but instead to a "lookalike" website *southchinapost[.]net*.



We attribute the domain name *southchinapost[.]net* to Cytrox's Predator spyware with high confidence. This domain name matched our fingerprint **F1** from our *PREDATOR IN THE WIRES* report; a website matching fingerprint **F1** was used to deliver a chain of iOS zero-day exploits, followed by a sample of Cytrox's Predator spyware, to a target in Egypt via network injection.

Additionally, we note that the *southchinapost[.]net* domain features in this recent report as attributed to Cytrox / Predator by researchers at Sekoia, pivoting from domains released in *PREDATOR IN THE WIRES*.

While we are not aware if anyone clicked on this link, we assess that if a user had clicked on the link, their phone could have been infected with Cytrox's Predator spyware. Like other mercenary spyware, Cytrox Predator infection could allow the spyware's operator to see almost everything on the user's device, including snooping on encrypted calls and messages. A recent analysis of leaked documentation by Amnesty International's Security Lab describes Predator's specific capabilities in more detail.

Based on a sample of Predator spyware that we captured in Egypt in September 2023, we outline part of the validation procedure that Predator uses to determine whether a user who clicked on a link should be infected (see: **Section 2**).

2. Predator Install Validation Process

Like similar mercenary spyware, after a target has navigated to a Predator infection link, either by clicking on the link, or by being forcibly redirected there through the use of network injection, Cytrox's Predator implements a series of validation checks to determine whether the Predator spyware should be installed on the target's device.

Some of these checks are implemented by the Predator installation server, and some are implemented by code that Predator runs on the user's device. While we do not have direct visibility into checks implemented on the Predator installation server, we were able to reverse engineer checks employed by a sample of Predator we captured in September 2023.

After the infection link delivers zero-day exploits to hack the device, but before Predator is installed, an eight-step validation program is executed on the device. If any of the validation steps fail, installation of Predator is aborted and telemetry is sent back indicating the specific failure reason.

Most of these checks seem designed to avoid infecting devices under active observation by security researchers. The validation also involves a rudimentary location check designed to avoid targeting American and Israeli devices. Such a check is likely to be highly approximative and may not correspond to a phone's actual location at time of infection. Note that the Predator installation server might implement further location checks, such as attempting to geolocate the IP address used by the user who clicks on the infection link. The server might decide to abort installation if the IP address is geolocated to certain regions.

These multi-layered checks highlight the difficulty for security researchers in obtaining the "final payload" of mercenary spyware. The spyware industry has evolved these checks over time, in response to several high-profile incidents where full spyware payloads were captured, such as our 2016 capture of NSO Group's Pegasus spyware, and our 2021 capture of Cytrox's Predator spyware.

The Eight Validation Steps

Step 1: Running Process Check

The validator checks the count of running processes that launched from the /private/var/tmp/ directory on the phone. The validator aborts if there is more than one such process. On an uncompromised phone, exactly zero processes should be running from this directory. Since Predator runs two processes from the /private/var/tmp/ directory, this could be a check to ensure that Predator has not already infected the phone. This check also might cause installation to fail if certain other types of spyware are present on the device.

Step 2: Check for Log Monitoring
The validator checks if the system log is actively being observed on the phone and aborts if so. Typically, only developers or security researchers would observe a phone's log.

Step 3: Rudimentary Location Check
The validator checks the locale selected on the phone. The locale consists of a language and country selected by the user. The user can change this at any time in their phone settings. Changing the locale changes the language displayed in the user interface, as well as various number formats (e.g., commas vs periods for decimal points), date formats, calendar type (e.g., Gregorian, Hijri, Jalali), units of measure (celsius vs fahrenheit), etc. If the country code of the locale is "IL" (Israel) or "US" (the United States), then the validator aborts. For many reasons, locale might not always correspond to the phone's physical location.

Step 4: Developer Mode Check
The validator checks if developer mode is enabled on the phone, and aborts if so.

Step 5: Jailbreak Detection
The validator checks if Cydia is installed and aborts if so. This might indicate that the phone has been jailbroken with a commodity jailbreak tool. A jailbreak tool could allow a security researcher to extract components of the spyware or exploits that could not be extracted from a normal device.

Step 6: Monitoring check
The validator checks if any "unsafe" processes are running and aborts if so. The hardcoded list of "unsafe" processes include apps that a security researcher might run, such as *tcpdump* and *netstat* to observe network traffic, sshd to access files on the device, *frida-server* to inject code into processes, and *checkra1nd*, a jailbreak tool. The list of "unsafe" processes also includes three mobile security apps.

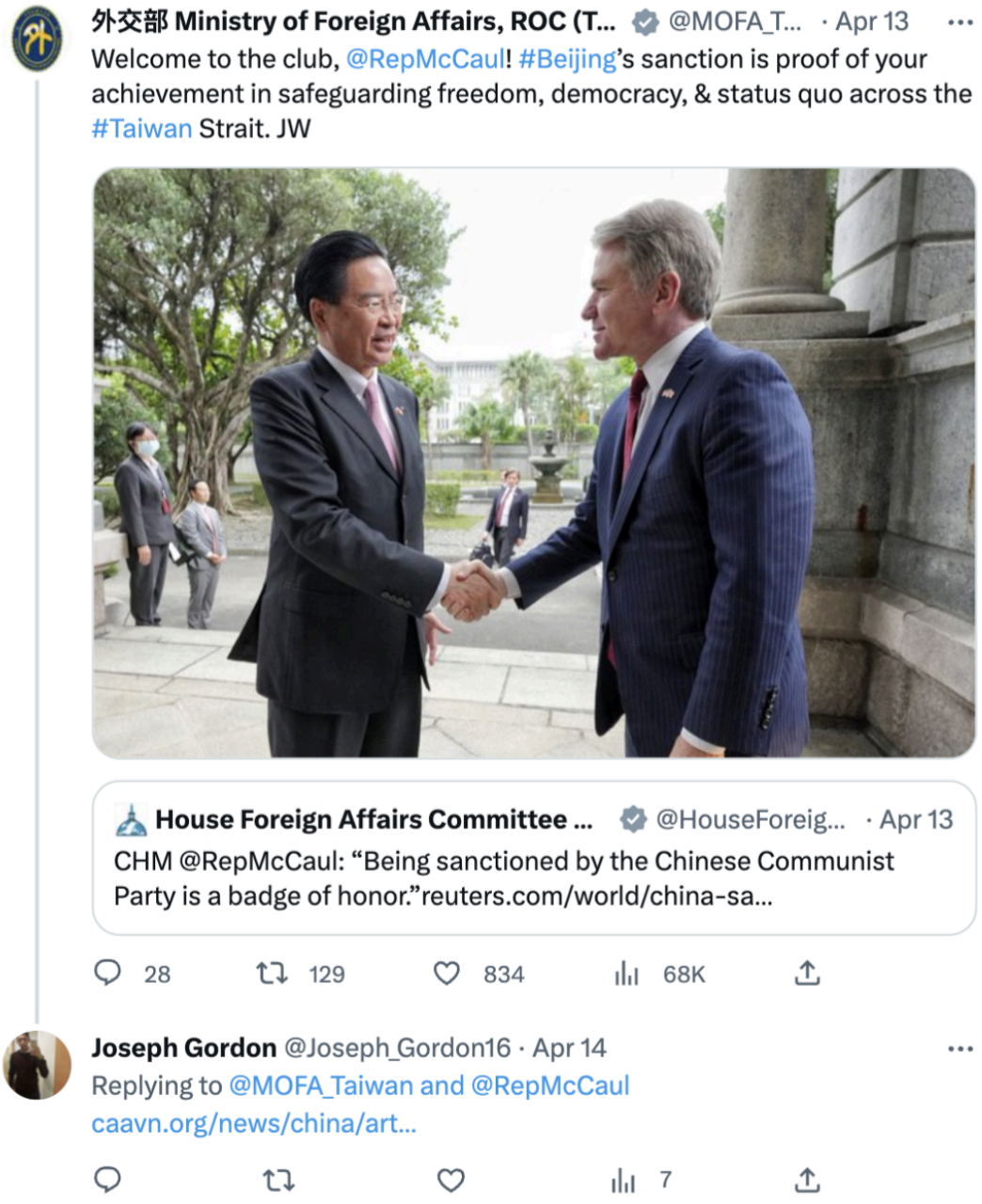
Step 7: Proxy Check
The validator checks if the user has configured a "proxy" for their Internet traffic and aborts if so. A proxy might be used by security researchers to intercept encrypted traffic from the device.

Step 8: MiTM Check
Finally, the validator checks if any additional root Certificate Authorities have been installed and aborts if so. The use of additional root Certificate Authorities could indicate that a security researcher is attempting to intercept encrypted traffic from the device.

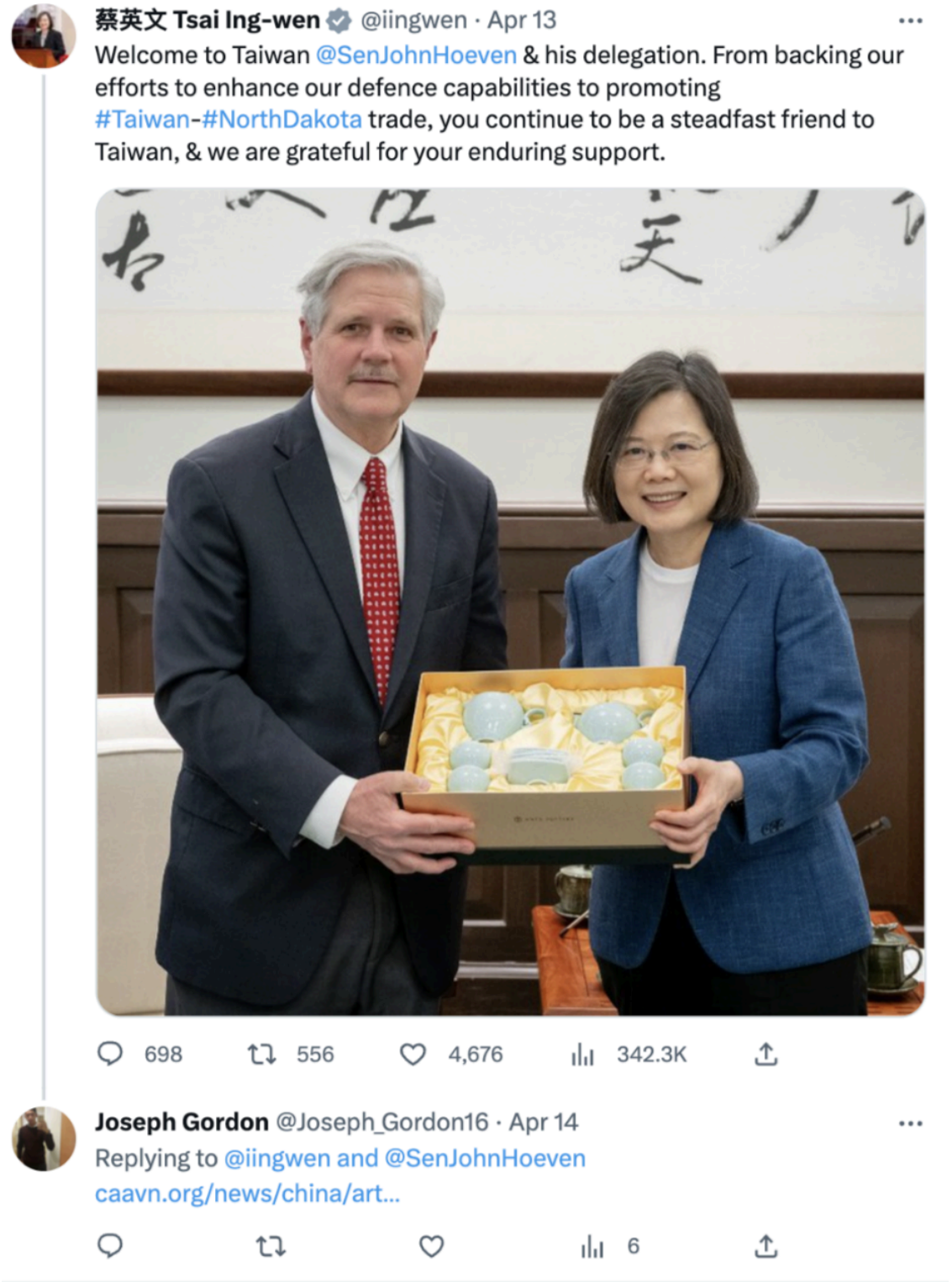
If all steps are successful, barring other failure conditions, we judge that the Predator infection would complete.

3. Extensive *REPLYSPY* Targeting of Officials, Media & Civil Society

We note a wider range of suspected targeting by the ***REPLYSPY*** actor, in line with the findings of Amnesty's Security Lab detailed here. For example, "Joseph Gordon"repeatedly replied to tweets mentioning multiple additional elected US officials.



Notably the targeting occurred on themes related to Taiwan with links to URLs on the domain name *caavn[.]org*.



Amnesty International's Security Lab attributes *caavn[.]org* to Cytrox during the period that the links were shared, and provides an extensive list of additional targeting and analysis, including the targeting of journalists, European and other elected and appointed officials, and commentators on Southeast Asian issues. We observed the *caavn[.]org* domain name pointing to an IP address that **F1**-matching domains pointed to.

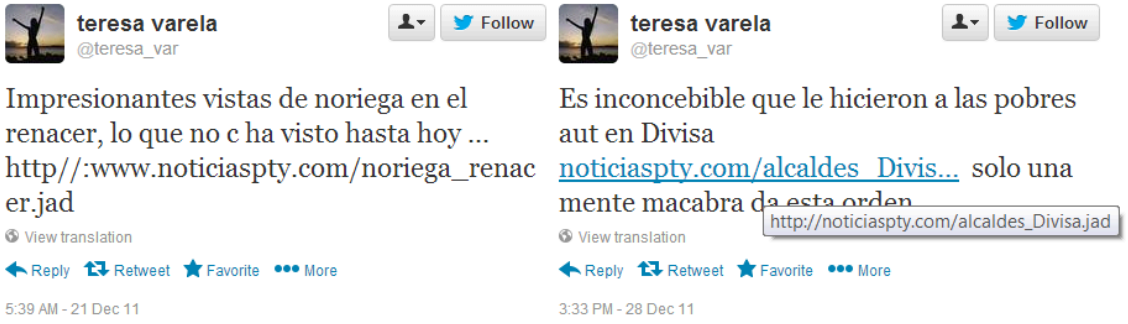
Amnesty's Security Lab highlights that the primary ***REPLYSPY*** Twitter / X account shows signs of alignment with the interests of the government of Vietnam, which was recently revealed by *Der Spiegel* as part of the

Predator Files to be a Cytrox customer, having purchased Predator for 5.6 million Euros for 2 years. The Citizen Lab also noted signs of a Vietnamese nexus with the primary observed account.

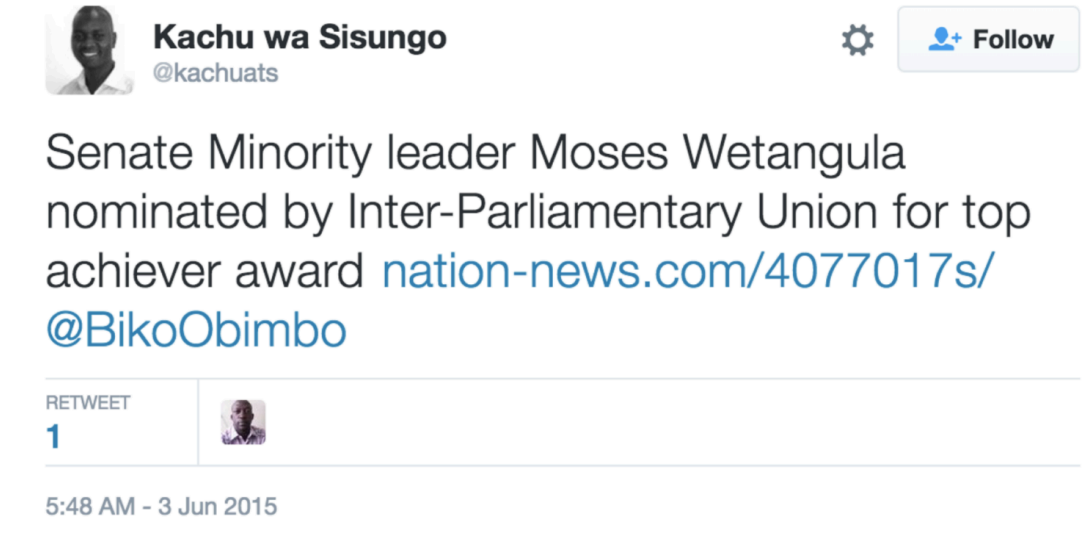
Public Posts for Mercenary Spyware Targeting: Rare

Unsurprisingly, we rarely observe mercenary spyware links being delivered on public facing social media posts. Posting links publicly entails a substantial risk of discovery and exposure, as well as the possibility of a link being clicked by an unintended target. Because spyware is often priced on a per-infection basis, it is often undesirable for operators to risk installation on unintended targets by posting infection links publicly. The use of such replies likely points to a lack of professionalism or of concern for the possibilities of getting caught.

Nevertheless, we have identified several other limited cases of spyware infection links distributed publicly via Twitter. One notable case is from 2011, where we documented a Twitter account posting a Panama-linked Hacking Team RCS infection link.



Additionally, in 2015, we observed a Pegasus infection link in a Tweet mentioning Kenya's then-Senate Minority Leader Moses Wetangula. Pegasus is developed and sold by NSO Group.



The fact that ***REPLYSPY*** extensively used this technique in 2023 is somewhat surprising, and might point to a lack of professionalism, a failure by Cytrox / Intellexa to direct customer behavior, or a perception by the customer that the targeting would be consequence-free.

Official Targeting With Mercenary Spyware: Proliferation's Price-tag

The pervasive targeting of human rights defenders, dissidents, and journalists with mercenary spyware is undeniable and extensively documented. In recent years, a second category of targeting has emerged: foreign espionage activities. This activity is extensive and targets some of the world's largest democracies.

When the US added Cytrox and Intellexa to the Entity List on July 18, 2023, they found that the companies had engaged in activities contrary to the national security interests of the United States and to human rights. These latest cases of officials targeted over Twitter suggest that the threat to US national security posed by these companies and the actions of their customers are direct. They join a growing list of cases of officials targeted with spyware. In March 2023, the US confirmed that at least 50 officials stationed in 10 countries were targeted with mercenary spyware.

While reports of the targeting of US officials are relatively recent, past reporting and investigations, notably including the Pegasus Project, have underlined just how extensively mercenary spyware is used as a tool of espionage against officials. That project found that at least ten prime ministers and three presidents had been potentially selected for targeting with Pegasus. The Citizen Lab has also reported on extensive evidence of Pegasus spyware infections in governmental networks, for example, finding an infection at 10 Downing Street, and the UK's Foreign Commonwealth and Development Office.

This latest case of targeting on Twitter/ X includes replies to posts from civil society as well as elected officials around the world. If indeed an element of the government of Vietnam is responsible for ***REPLYSPY***, the targeting of civil society and foreign espionage attempts targeting the US, EU and other countries are unsurprising. As described by *Der Spiegel*, Intellexa executives and their benefactors sought and won contracts with government clients that are widely known abusers of human rights worldwide.

Information acquired by the Predator Files project reveals a flagrant disregard for accountability mechanisms, as well as those mechanisms' inherent weaknesses. Rather than undertake any serious due diligence, Intellexa executives and their allies sought instead to wittingly skirt export controls to sell surveillance technology to regimes they knew were likely to abuse them. The complicity of senior European business executives and politicians in these endeavors shows why regulation of the mercenary spyware market is so difficult to accomplish. Notably, German agencies are reported to be clients of Intellexa; Germany is also not among the 11 countries that recently pledged to work collectively to counter the proliferation and misuse of commercial spyware.

Read More Citizen Lab Research on Cytrox's Predator Spyware:

The Citizen Lab has conducted several investigations into Predator spyware.

2021:Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware This report describes the first discovery of a Predator infection in the wild on a device also infected with NSO Group's Pegasus spyware.

2022: Citizen Lab analyses confirmed Predator infections on the devices of Greek journalist Thanasis Koukakis and former Meta manager, Artemis Seaford, among others.

2023: Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions. This report describes how network injection techniques were used to target Ahmed Eltantawy, resulting in the co-discovery with Google's Threat Analysis Group of the iOS exploit chain CVE-2023-41991, CVE-2023-41992, CVE-2023-41993.

Source: https://citizenlab.ca/2023/10/predator-spyware-targets-us-eu-lawmakers-journalists/