censys

How Censys Helped Citizen Lab Expose Mercenary Spyware Vendor Candiru

Attacker Profile

Candiru is a private sector offensive actor known for selling malware to governments. Their core product offering is spyware that can be installed through a number of infection vectors on a target's Apple, Windows, or Android device. Candiru claims that their products are "untraceable," which makes finding domains, certificates, and other C&C infrastructure affiliated with their software especially challenging. In recent years, Candiru spyware has attracted international attention due to its active use in targeting human rights defenders, journalists, and political activists.

"The powerful search functionality and extensive historical data made Censys great to use for attribution. Censys is used in almost every investigation we do."

Bill Marczak
Research Fellow at Citizen Lab

Citizen Lab Launches an Investigation Into Candiru

Citizen Lab is a University of Toronto research institute at the inter-section of human rights and information technology that focuses on research, policy, and advocacy. One unique aspect of Citizen Lab's mission is their investigations into the technical practices used to target activists and journalists. Bill Marczak, a Senior Research Fellow at Citizen Lab, along with other researchers have uncovered and unraveled numerous attacks using Censys, including the first-ever iPhone zero-day remote jailbreak seen in the wild. Most recently, Citizen Lab investigated Candiru. Alongside other researchers at Citizen Lab, Bill decided to pursue a formal investigation, publishing a detailed report on the company's practices that was picked up by The New York Times and other news organizations.

Citizen Lab's Threat Hunting Goal

Citizen Lab used Censys' Universal Internet DataSet that details IPv4 hosts and services as well as Censys' certificate dataset to map Candiru's command and control (C&C) infrastructure and to understand the websites that Candiru's spyware has been used to target, ultimately undercovering that Candiru is actively targeting members of civil society, academics, and the media. In the words of Bill Marczak, "We were curious about mapping out command and control infrastructure — IPs, domains, certificates — with the ultimate goal of understanding Candiru's global footprint."

What Citizen Lab Achieved

- **Mapped Candiru's C2 Infrastructure**
  Citizen Lab identified a certificate for candirusecurity.com, which allowed them to identify IP addresses historically associated with Candiru, and ultimately develop a fingerprint to find the websites that Candiru was attempting to impersonate.

- **Microsoft Threat Intelligence Center (MSTIC) Identified Two Privilege Escalation Vulnerabilities**
  Citizen Lab shared a signature that allowed Microsoft to identify two previously undisclosed privilege escalation vulnerabilities exploited by Candiru malware: CVE-2021-31979 and CVE-2021-33771, as well as identify more than 100 other human rights defenders, journalists, activists, and politicians who were targeted by Candiru's spyware.

How Censys Universal Internet Dataset and Search Was Used to **Understand the Impact of Candiru**

What certificates are affiliated with the candirusecurity[.]com domain name?

Citizen Lab found a self-signed certificate on Censys Search that was associated with Candiru. Their team knew to search for a specific domain: "candirusecurity[.]com" because they had found a 2015 corporate registration filing associated with Candiru. The registration included an email with the same domain: "amitn@candirusecurity[.]com." This certificate finding was significant because it allowed the team to pivot to and uncover other attacker infrastructure using the historical Censys IPv4 dataset.

Which IPs were serving the certificate and what did that indicate about the targets, their geographies, and Candiru's methods?

Citizen Lab queried the Censys IPv4 dataset to locate the IP addresses that were serving the certificate and potentially affiliated with Candiru. The team iterated between IPv4 hosts and certificates, ultimately surfacing certificates for over 750 websites that Candiru spyware infrastructure was impersonating. These included sites belonging to to well known advocacy organizations like amnestyreports[.]com and activist organizations like blacklivesmatters[.]info. Other less-well known sites were country specific and linked to Saudi Arabia, Russia, and Armenia. These provided hints to where targets could be located and methods currently used to entrap them.

Citizen Lab was also able to find an IP address via Censys that belonged to a victim of the spyware. Bill Marczak, a Research Fellow at Citizen Lab, stated, "Censys data was a critical part of the investigation because it helped us find the victim and recover the spyware sample."

Through this research, Citizen Lab was able to pass on samples to Microsoft that allowed the Microsoft Threat Intelligence Center (MSTIC) to pivot off these IoCs and find the exploits: CVE-2021-31979 and CVE-2021-33771 as well as 100 victims of spyware in many countries.

Mapping Candiru's Command and Control Infrastructure

Self-signed TLS Certificate
amitn@candirusecurity[.]com

6 IP Addresses
Returned this certificate

4 of these IPs
Returned a new certificate

Fingerprint CF1

42 Certificates
Matched Fingerprint CF1

6 IP Addresses
Matched Fingerprint CF1

Additional Certificates
Revealed by the 6 IPs

Fingerprint CF2

Why Did Citizen Lab Choose Censys?

- **BigQuery, Search, and Raw Data Access**
  Censys provides access to hundreds of terabytes of historical Internet scan data through an online search interface, high-speed lookup API, Google BigQuery datasets, and raw data downloads.
- **Scalable, Differentiated Data on Hosts and Certificates**
  Censys has the broadest coverage of both IPv4 hosts and certificates. Censys offers a dataset of 5 billion parsed and browser-validated X.509 certificates in addition to detailed records about IPv4 hosts and their service configuration going back six years.
- **Speed and Accuracy**
  Censys provides the freshest data through scanning more than 100 protocols across the top 3,500 ports on the full IPv4 address space every 10 days and the top 100 ports daily.

> **Censys structures Internet data in a way that's easy to understand and query. Without regular expression queries and the ability to query specific fields, we wouldn't have been able to develop or search for other hosts that matched our signature.**

Bill Marczak,
Research Fellow at Citizen Lab

censys

VISIT
censys.com

CONTACT
hello@censys.com

Censys' mission is to be the one place to understand everything on the internet. Frustrated by the lack of trustworthy Internet intelligence, we set out to create the industry's most comprehensive, accurate, and up-to-date map of the Internet. Today, Censys delivers real-time Internet intelligence and actionable threat insights to global governments, over 50% of the Fortune 500, and leading threat intelligence providers worldwide.