Candiru's Spyware:How It Works And Attacking Journalists,Activists And Many More

eyesonlife.org/Features/Science_and_Technology/Candirus_Spyware_How_It_Works_And_Attackng_Journalists_Activists_And_Many_More

July 13, 2021

Directory

17-07-2021 Saturday 15:00

_According to cybersecurity researchers at the University of Toronto’s Citizen Lab, recently at least 100 activists, journalists and government dissidents across 10 countries were targeted with a spyware produced by an Israeli company called Candiru, which tracks illegal hacking and surveillance.

The researchers confirmed, using a pair of vulnerabilities in Microsoft Corp.’s Windows, cyber operatives operating in Saudi Arabia, Israel, Hungary, Indonesia and elsewhere purchased and installed remote spying software made by Candiru.

Cristin Goodwin, general manager of Microsoft’s Digital Security Unit, said the tool was used in precision attacks against targets’ computers, phones, network infrastructure and internet-connected devices.

According to a Microsoft blog published on Thursday, Microsoft was alerted to these attacks by researchers at Citizen Lab, and after weeks of analysis, the company released patches on July 13 for a pair of Windows vulnerabilities believed to be the point of entry for the spyware.

Microsoft doesn’t name Candiru but instead refers to an Israel-based private sector offensive actor it calls Sourgum. Candiru didn’t immediately respond to a message seeking comment.

While the company’s current name is Saito Tech Ltd, we will refer to them as 'Candiru' as they are most well known by that name.

Candiru is a secretive Israel-based company that sells spyware exclusively to governments. Reportedly, their spyware can infect and monitor iPhones, Androids, Macs, PCs, and cloud accounts.

Citizen lab identified a politically active victim in Western Europe and recovered a copy of Candiru’s Windows spyware.

Microsoft observed at least 100 victims in Palestine, Israel, Iran, Lebanon, Yemen, Spain, United Kingdom, Turkey, Armenia, and Singapore. Victims include human rights defenders, dissidents, journalists, activists, and politicians.

Here we will try a short brief on the technical overview of the Candiru spyware's persistence mechanism and some details about the spyware's functionality accordiing to a research by citizen lab. Candiru has made efforts to obscure its ownership structure, staffing, and investment partners.

The company known as Candiru, based in Tel Aviv, Israel, is a mercenary spyware firm that markets untraceable spyware to government customers. Their product offering includes solutions for spying on computers, mobile devices, and cloud accounts.

How to identify

Candiru's spyware was persistently installed on the computer via COM hijacking of the following registry key:

HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32

Normally, this registry key's value points to the benign Windows Management Instrumentation wmiutils.dll file, but the value on the infected computer had been modified to point to a malicious DLL file that had been dropped inside the Windows system folder associated with the Japanese input method (IMEJP) C:\WINDOWS\system32\ime\IMEJP\IMJPUEXP.DLL.

This folder is benign and included in a default install of Windows 10, but IMJPUEXP.DLL is not the name of a legitimate Windows component.

To identify the websites used by Candiru's spyware, citizen lab developed four fingerprints and a new Internet scanning technique. They searched for the historical data from Censys and conducted their own scans in 2021.

They identified at least 764 domain names that we assess with moderate-high confidence to be used by Candiru and its customers. Examination of the domain names indicates a likely interest in targets in Asia, Europe, the Middle East, and North America.

A leaked Candiru project proposal published by TheMarker shows that Candiru's spyware can be installed using a number of different vectors, including malicious links, man-in-the-middle attacks, and physical attacks.

The Candiru systems operated from Saudi Arabia, Israel, UAE, Hungary, and Indonesia, among other countries.

A vector named Sherlock is also offered, that they claim works on Windows, iOS, and Android. This may be a browser-based zero-click vector.

Like many of its peers, Candiru appears to license its spyware by number of concurrent infections, which reflects the number of targets that can be under active surveillance at any one instant in time. Like NSO Group, Candiru also appears to restrict the customer to a set of approved countries.

How it Works

Using Internet scanning citizen lab identified more than 750 websites linked to Candiru's spyware infrastructure. Among them, many domains masquerading as advocacy organizations such as Amnesty International, the Black Lives Matter movement, as well as media companies, and other civil-society themed entities.

After analyzing the spyware with the help of Microsoft Threat Intelligence Center (MSTIC), it discovered the CVE-2021-31979 and CVE-2021-33771 by Microsoft, two privilege escalation vulnerabilities exploited by Candiru. Microsoft patched both vulnerabilities on July 13th, 2021.

The IMJPUEXP DLL file has eight blobs in the PE resources section with identifiers 102, 103, 105, 106, 107, 108, 109, 110. The DLL decrypts these using an AES key and IV that are hardcoded in the DLL. Decryption is via Windows CryptoAPI, using AES-256-CBC.

When Windows boots, it automatically loads the Windows Management Instrumentation service, which involves looking up the DLL path in the registry key, and then invoking the DLL.

IMJPUEXP.DLL decrypts and loads the AgentService.dat file whose path is in resource 103, using the same AES key and IV, and decompresses it via zlib.

AgentService.dat file then loads the file in resource 105, KBDMAORI.dat, using a second AES key and IV hardcoded in AgentService.dat, and performs the decryption using a statically linked OpenSSL.

Decrypting KBDMAORI.DAT yields a file with a series of nine encrypted blobs, each prefixed with an 8-byte little-endian length field. Each blob is encrypted with the same AES key and IV used to decrypt KBDMAORI.DAT, and is then zlib compressed.

Candiru's Windows payload appears to include features for exfiltrating files, exporting all messages saved in the Windows version of the popular encrypted messaging app Signal, and stealing cookies and passwords from Chrome, Internet Explorer, Firefox, Safari, and Opera browsers.

Microsoft's analysis also established that the spyware could send messages from logged-in email and social media accounts directly on the victim's computer.

This could allow malicious links or other messages to be sent directly from a compromised user's computer. Proving that the compromised user did not send the message could be quite challenging.

Candiru spyware is part of a thriving private industry selling technology to governments and authoritarian leaders so they can gain access to the communications of private citizens and political opposition.

Another Israeli company, NSO Group Ltd., has been accused of providing spyware to repressive governments that have used it to snoop on journalists and activists.

NSO has maintained that it sells its technology exclusively to governments and law enforcement as a tool against terrorism and crime. In a report published on June 30, the Group said it refuses to sell spyware to 55 countries and has taken steps to curb misuse by customers.

For 16 million euros ($18.9 million), Candiru's clients can attempt to compromise an unlimited number of devices but are limited to actively tracking only 10 at a time, according to Citizen Lab. For an extra 1.5 million euro ($1.8 million), buyers can monitor an additional 15 victims.

Candiru has clients in Europe, Russia, the Middle East, Asia and Latin America, according to the Israeli newspaper Haaretz. Local news organizations have reported contracts in Uzbekistan, Saudi Arabia, the United Arab Emirates, Singapore and Qatar, according to Citizen Lab's report.

Candiru's clients are restricted to operating only in agreed upon territories, according to Citizen Lab. The company's clients sign contracts that limit operations outside the U.S., Russia, China, Israel and Iran, according to the report.