# Spyware campaign targeted journalists, activists: researchers

15 July 2021

Researchers say a sophisticated spyware campaign was used to target activists, journalists and others.

A spyware campaign using tools from a secretive Israeli firm was used to attack and impersonate dozens of human rights activists, journalists, dissidents, politicians and others, researchers said Thursday.

Statements from Microsoft security researchers and the University of Toronto's Citizen Lab said powerful "cyberweapons" were being used in precision attacks targeting more than 100 victims around the world.

Microsoft said it patched this week the vulnerability exploited by the group, known by the names Candiru and Sourgum.

Citizen Lab said in a blog post that "Candiru is a secretive Israel-based company that sells spyware exclusively to governments," which can then use it to "infect and monitor iPhones, Androids, Macs, PCs, and cloud accounts."

"We found 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," Citizen Lab said.

Microsoft observed at least 100 victims in the Palestinian territories, Israel, Iran, Lebanon, Yemen, Spain, Britain, Turkey, Armenia and Singapore.

The US tech firm said it moved to thwart the attacks with Windows software updates that prevent Candiru from delivering its malware.

"Microsoft has created and built protections into our products against this unique malware, which we are calling DevilsTongue," a Microsoft statement said.

"We have shared these protections with the security community so that we can collectively address and mitigate this threat."

According to Microsoft, DevilsTongue was able to infiltrate popular websites such as Facebook, Twitter, Gmail, Yahoo and others to collect information, read the victim's messages and retrieve photos.

"DevilsTongue can also send messages as the victim on some of these websites, appearing to any recipient that the victim had sent these messages," said the statement from Microsoft Threat Intelligence Center.

"The capability to send messages could be weaponized to send malicious links to more victims."

Citizen Lab researchers found evidence the spyware can exfiltrate private data from a number of apps and accounts, including Gmail, Skype, Telegram and Facebook.

It can also capture browsing history and passwords, as well as turn on the target's webcam

and microphone, according to the findings.

Citizen Lab said the Israeli firm's current name is Saito Tech Ltd, and that it has some of the same investors and principals as NSO Group, another Israeli firm under scrutiny for surveillance software.

© 2021 AFP

APA citation: Spyware campaign targeted journalists, activists: researchers (2021, July 15) retrieved 21 May 2022 from https://techxplore.com/news/2021-07-spyware-campaign-journalists-activists.html

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*