

Skype chats compromised Syrian rebels: researchers

February 2 2015

Syrian opposition groups lost critical information when its members fell victim to a "femme fatale" scheme using Skype chats that injected computers and phones with malware, researchers said Monday.

The security firm FireEye said it uncovered the hacking scheme that stole tactical battle plans, geographical coordinates, information on weapons and other key data in a period from November 2013 to January 2014, and possibly longer.

The hackers lured victims into online chats with attractive female avatars, eventually delivering a malware-laden photo, that allowed the operators of the scheme to steal "scores of documents that shed valuable insight into [military operations](#) planned against President (Bashar al) Assad's forces," FireEye said in a report.

"Sometimes, the threat group would take whole sets of files pertaining to upcoming large-scale military operations. These included correspondence, rosters, annotated satellite images, battle maps, orders of battle, geographic coordinates for attacks, and lists of weapons from a range of fighting groups."

The group asked its targets about the device they used—computer or Android phone—probably to deploy malware specifically tailored to that device, FireEye said.

In addition to the military and political documents stolen, the group also

accessed the Skype databases of the victims to get contacts and [real time communications](#), "providing the threat actors with an inside view into the opposition's relationships and plans."

FireEye said it lacked sufficient information to determine the identity of the hackers or their ties to Assad's forces, but noted that "we have some indications that the group may be resourced and/or located outside of Syria."

"We found the activity focused on the Syrian opposition that shows another innovative way threat groups have found to gain the advantage they seek," said Nart Villeneuve, a researcher at FireEye.

"While we cannot positively identify who is behind these attacks, we know that they used social media to infiltrate victims' machines and steal military information that would provide an advantage to President Assad's forces on the battlefield."

© 2015 AFP

Citation: Skype chats compromised Syrian rebels: researchers (2015, February 2) retrieved 18 April 2024 from <https://phys.org/news/2015-02-skype-chats-compromised-syrian-rebels.html>

<p>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.</p>
--