'Honey trap' hackers stole Syria rebel plans

BEIRUT, LEBANON: Hackers targeted Syrian opposition members with online "honey traps," posing as female supporters to steal battle plans and the identity of defectors, a US security firm said Monday...

Beirut from space... The report says that as computers were shared, hacking just one would enable the hackers to access information on a number of users. (Image: NASA)

A report produced by US cyber security firm FireEye describes how the hacking operations in late 2013 and early 2014 targeted Syrian opposition fighters, media activists and humanitarian aid workers.

The group said it was unclear whether the information had been passed onto the Syrian government, and who the hackers were.

But the hacked material included a detailed opposition military plan to recapture the town of Khirbet Ghazaleh, strategically located in southern Daraa province, in 2013.

"The hackers stole a cache of critical documents and Skype conversations revealing the Syrian opposition's strategy, tactical battle plans, supply needs, and troves of personal information and chat sessions," the report said.

The hacking provided "actionable military intelligence for an immediate battlefield advantage" in the case of the planned Khirbet Ghazaleh attack.

Multiple users, multiple victims

It captured "the type of insight that can thwart a vital supply route, reveal a planned ambush and identify and track key individuals." Despite the high-tech tools used in the attack, the hackers also relied on a well-worn tactic: the "honey trap."

Targets were contacted on the chat and online phone service Skype by hackers posing as pro-opposition women.

They would ask the target whether they were on a smartphone or computer, apparently in a bid to tailor their attacks.

Then the hackers would send the target a photo of themselves loaded with malware that penetrated their personal files and stole information. The method was particularly fruitful because Syrian opposition members were often sharing computers, meaning one machine yielded information from multiple victims.

Most of the data stolen was created between May 2013 and December 2013, but some of the stolen Skype chat logs went back to 2012 and others included information from as recently as January 2014.

The hackers also used other tactics, including creating fake social media accounts and Syrian opposition websites that encouraged visitors to click on links that would infect their computers.

In May 2013, regime troops stormed Khirbet Ghazaleh, which was rebel-held at the time and being used to block the highway between Damascus and Daraa.

The report was unable to identify where the hackers were based, or who they might have reported to, But it noted that the hackers' servers were based outside of Syria and they used tools and tactics that were different from other Syrian hackers.

Syria's conflict has involved other documented cases of cyberwarfare, by both pro-regime and opposition activists.

Some of the most high-profile include attacks by the so-called Syrian Electronic Army, a group of pro-government hackers who have attacked websites and social media accounts belonging to media outlets and politicians.

Source: AFP, via I-Net Bridge

For more, visit: https://www.bizcommunity.com