'Honey trap' hackers stole Syria rebel plans

February 2 2015, by Sara Hussein

A rebel fighter looks at his smartphone lying on a sofa on October 23, 2014, in Bustan Pasha neighbourhood of Syria's northern city of Aleppo

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

The report, by US cybersecurity firm FireEye, tracked hacking operations in late 2013 and early 2014 that targeted Syrian opposition fighters, media activists and humanitarian aid workers.

FireEye said it was unclear whether the information stolen from the Syrian opposition had been passed onto the Syrian government and who the hackers were working for.

But the hacked material included a detailed opposition military plan for an attack in 2013 on the town of Khirbet Ghazaleh, strategically located in southern Daraa province.

The town had been under rebel control but was seized by regime troops in May 2013. Rebels have been unable to recapture it since.

"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.

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 they would send their victim a photo of themselves loaded with

malware that penetrated their personal files and stole information.

The method was particularly effective because Syrian opposition members were often sharing computers, meaning one machine yielded information from multiple victims.

Stealth cyber-war

The material stolen covered extraordinary levels of detail, including the blood types of fighters and the timing of a handover of anti-tank missiles.

But not all of it related to warfare, with information about refugees, opposition media strategy and the inner workings of opposition political structures also included.

Most of the stolen material was created between May 2013 and December 2013, though some of it dated back to 2012 and 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.

FireEye was unable to identify where the hackers it tracked were based, but it noted that their servers were outside of Syria and their tools and tactics differed from previous Syrian hackers.

The report's revelations are just the latest evidence of the stealth cyberwar that has accompanied the fighting in Syria's bloody conflict.

Pro-government hackers identifying themselves as the Syrian Electronic Army have carried out high-profile attacks against the websites and

social media accounts of media outlets and politicians.

And in 2012, a British newspaper published what it said were 3,000 emails sent by President Bashar al-Assad and his wife, obtained by opposition hackers with the help of a government mole.

Sami Saleh, an opposition activist and hacker using a pseudonym, said such examples were rare because the opposition was generally too poorly-equipped and -backed to carry out major hacking operations.

"We mostly carry out defensive operations," he told AFP, describing multiple cases where opposition commanders and politicians were targeted by hackers.

In one case, a commander in northwestern Idlib province downloaded a file meant to contain military maps, accidentally compromising his computer.

"The cyber-war is about half the war, without exaggeration," Saleh said.

Citation: 'Honey trap' hackers stole Syria rebel plans (2015, February 2) retrieved 12 May 2024 from https://phys.org/news/2015-02-honey-hackers-stole-syria-rebel.html