North Korean hackers infiltrate Chile's ATM network after Skype job interview

zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/

Home Innovation Security

Redbanc employee applied for a LinkedIn job and got a call from the world's most active hacker crews.

Written by Catalin Cimpanu, Contributor on Jan. 15, 2019

-
-
-
-
-

A Skype call and a gullible employee was all it took for North Korean hackers to infiltrate the computer network of Redbanc, the company that interconnects the ATM infrastructure of all Chilean banks.

Prime suspects behind the hack are a hacker group known as Lazarus Group (or Hidden Cobra), known to have associations to the Pyongyang regime, is one of the most active and dangerous hacking groups around, and known to have targeted banks, financial institutions, and cryptocurrency exchanges in the past years.

Lazarus' most recent attack took place at the end of December last year but only came to the public's attention after Chilean Senator Felipe Harboe called out Redbanc on Twitter last week for not disclosing its security breach.

The company, which has direct lines into the networks of all Chilean banks, formally admitted to the hack a day later in a message posted on its website, but that announcement didn't include any details about the intrusion.

However, a day after Redbanc's admission, an investigation conducted by Chilean tech news site *trendTIC* revealed that the financial firm was the victim of a serious cyber-attack, and not something that could be easily dismissed.

According to reporters, the source of the hack was identified as a LinkedIn ad for a developer position at another company to which one of the Redbanc employees applied.

The hiring company, believed to be a front for the Lazarus Group operators who realized they baited a big fish, approached the Redbanc employee for an interview, which they conducted in Spanish via a Skype call.

trendTIC reports that during this interview, the Redbanc employee was asked to download, install, and run a file named ApplicationPDF.exe, a program that would help with the recruitment process and generate a standard application form.

Image: Flashpoint

But according to an analysis of this executable by Vitali Kremez, Director of Research at Flashpoint, the file downloaded and installed PowerRatankba, a malware strain previously linked to Lazarus Group hacks, according to a Proofpoint report published in December 2017.

The malware, Kremez said, collected information about the Redbanc employee's work PC and sent it back to a remote server. Collected information included the PC's username, hardware and OS details, proxy settings, a list of current processes, if the infected host had RPC and SMB open file shares, and the status of its RDP connection.

The collected information would have been able to tell the hackers what computer they infected, and later decide if they'd want to deliver a second stage payload in the form of a more intrusive PowerShell script.

The Redbanc incident is yet another example of how one worker clicking on the wrong link or running the wrong file can result in a major security breach, and how one hacked PC or laptop can lead to an entire network getting compromised.

Previously, according to an indictment by US authorities, Lazarus Group hackers have been accused of attempting to steal money from Banco de Chile, a local Chilean bank.

Cybercrime and malware, 2019 predictions

More cybersecurity news: