Flaw found in Comcast's XFINITY home security system

2 million sets of personal records stolen in 2015 Japanese cyber-attacks

Blackphone given black eye by vulnerability discovery

December 2015 Issue

Editorial

Let's just call it "The era of IT security"

Subscribe

Archive

Tom Reeve

January 07, 2016

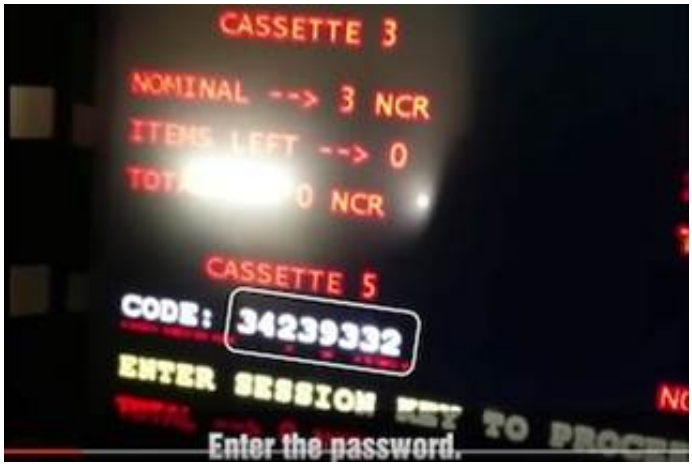
Eight arrested in eastern Europe over ATM malware attacks

Share this article:

- facebook
- twitter
- linkedin

Europol has announced the takedown of an international criminal gang believed to be behind a series of ATM malware attacks dating back to at least 2014.

Said to be one of the first operations of this type in Europe, it resulted in multiple house searches and arrests in Romania and the Republic of Moldova.



Tyupkin ATM trojan

Using malware dubbed Tyupkin, the suspects were allegedly able to empty cash from ATM machines on demand following the successful installation of a trojan. Called "ATM jackpotting", the exploit allowed attackers to empty infected machines by issuing commands via the machine's pin pad.

The malware was identified in 2014 by Kaspersky Lab following a request from a financial institution to investigate multiple attacks in eastern Europe. At the time of the investigation, Kaspersky reported that it had found the malware on more than 50 ATMs at banks in eastern Europe, but based on listings at VirusTotal, it was convinced that the virus had been deployed in the US, India, China, Russia, Israel, France and Malaysia.

However, according to a video posted on YouTube, the affected manufacturer may be NCR.

We reported in March 2015 that the Russian Ministry of Internal Affairs had made the identification of the Tyupkin malware gang a priority as they targeted an increasing number of ATMs in the country.

Kaspersky said that the attackers were able to install the malware via a bootable CD after gaining physical access to the PC inside the cash dispenser.

The malware enabled users to check the amount of cash in each cash cassette in the machine and dispense up to 40 notes at a time. It also had its own security built in by requiring the user to enter a session key based on a random seed and a secret algorithm before it would accept any commands.

The criminal investigation was conducted by Romanian National Police and the Directorate for Investigating Organised Crimes and Terrorism (DIICOT) assisted by Europol, Eurojust and other European law enforcement authorities.

- 0 Comments
- Email
- Print

You must be a registered member of SC Magazine to post a comment.
Click here to login | Click here to register

Sponsored Links