Who Needs Hackers?

Michael Barwise

As a rule I don't comment on unproven allegations, but this time I'm breaking my rule. According to a District of New Hampshire indictment, four Romanians are accused of ripping off credit cards remotely from a couple of hundred US retail outlets including Subway restaurant franchises. Allegedly, they scanned the internet for vulnerable POS terminals and then introduced backdoors that allowed them to filter off transaction details.

It's important to note that everything above and all of what follows is allegation only. The case has not been heard and the presumption of innocence is paramount. But I'm not actually very interested in the alleged crime. I am extremely interested, though, in how card transaction systems supposedly compliant with PCI security requirements (and necessarily therefore regularly penetration tested) could be located by scanning the internet, particularly as these were physical, not online, points of sale. I'm also interested in how, having been discovered, they could be illicitly accessed. What the alleged perpetrators might have done once they had achieved this (if they indeed did so) is much less important than the possibility that the equipment was so exposed and penetrable.

Information - even supposition - are currently in short supply. The indictment itself is silent on any means of initial illicit access to the POS terminals. But Wired, SC Magazine and DataBreaches.net all suggest that this was probably accomplished via remote management software installed on the computers supporting the POS terminals that fell victim. Wired compares this incident with a case in 2009 in which an attacker - also coincidentally Romanian - breached the POS systems of another restaurant chain. In that case it was alleged that the suppliers of the POS system had installed the PCAnywhere remote desktop system to facilitate their provision of support, but had applied a common user name and password to the installations at all the restaurant chain's 200 sites. It was even suggested that the defaults were "computer" and "password".

DataBreaches points out that *"Visa has repeatedly advised merchants to disable RDAs unless absolutely necessary."* I would go further. If remote management is absolutely unavoidable, it must be enabled immediately before the legitimate management operation and disabled immediately afterwards, and at least the password (but preferably both the user name and password if technically possible) must be changed on a regular cycle regardless of whether they have been used for maintenance. Yes, that is arduous. It's meant to be. Every possible means must be employed to extinguish the desire for remote management facilities on retail financial transaction equipment. It must never be employed for mere convenience, and where it is employed it must be rigorously managed to ensure these all too frequent breaches cease to occur. We must also do whatever is necessary to make the regular security tests mandated by PCI DSS achieve something more than a tick in a box on the audit form. They seem to have failed here as they failed in the case of TJX and who knows how many other occasions.

Who needs hackers while our infrastructure is this wide open and our security reviews are essentially meaningless?

Originally appeared on the Infosecurity Network, December 2011