Retail Banker
INTERNATIONAL

Cyber attacks on banks: beware the wolf in sheep's clothing

12 September 2013

Banks spend plenty of time and effort on security measures to protect their physical premises. Sophisticated safes, cash handling protocols, security doors and smoke screens are all commonly deployed to protect cash in-branch, writes **Geoff Webb**

Perhaps partly as a result of these measures, branch networks are no longer the primary target for criminals. Over the last decade or so a more attractive target has emerged, and the thieves targeting banks have themselves evolved. Now if a person wants to steal from a bank, they're not limited to the amount of money held in a branch or an ATM.

Funds stolen from banks by cyber criminals now dwarf those of "traditional" bank robberies, and it's easy to see why. Cyber criminals assume a far lower burden of risk than their masked, swag-carrying cousins, and the potential gains are much greater.
One disruptive technique which has come to prominence recently is the Distributed Denial of Service (or DDoS) attack, in which a cyber criminal floods the bank's servers with requests to bring down its network. Analysts have identified several recent incidences in which criminals have used DDoS attacks as a diversion to distract IT security teams while they steal millions of dollars through fraudulent wire transfers. A DDoS attack does not need to bring down a network to succeed: even slowing a network can paralyse a trading floor. And while Internet Service Providers (ISPs) are usually effective at helping respond to DDoS attacks and should be brought in as soon as possible, focusing exclusively on the denial of service attack may mean that the main attack remains undetected.

Unlike the masked men walking into a branch, on the surface at least, savvy hackers can be almost indistinguishable from genuine employees. Once inside the perimeter, a cyber criminal will aim to elevate his authorisation levels to those of a privileged employee and use these clearances to steal data and other assets. For this reason there is little point in talking about insider and outsider threats in cyber security. Banks have to assume that their perimeters are already breached and that the outsider has become an insider; a wolf in sheep's clothing.

Banks have long focused on fraud as a major security concern online, but in fact the theft of data can be even more harmful. When a customer's personal financial information has been compromised and is being sold to criminals online, this is likely to convince even the most loyal customer to find a new bank. The financial and reputational damage can be enormous.

So banks need to ask themselves: now what? If we are inevitably compromised, how do we act? And how do we limit the impact of such a breach, protect corporate information and minimise business risk? Because IT teams might be looking for one bad actor in amongst 200,000 employees globally, finding such an attacker inside the perimeter might be akin to hunting a needle in a haystack.

Traditionally one response to attackers is to try to spot the tools a hacker is using, but this is misguided. It's too easy to build unidentifiable tools. Instead, the key to uncovering hackers lies in behaviour and activity monitoring. Are you seeing new traffic, a change in the time of activity, or data flowing in new ways? If banks are looking for these tell-tale signs they have a much better chance of spotting an attack.