20/6/2012

Intruz uzyskał dostęp do wewnętrznej sieci Citibanku

Autor: igH | Tagi: atak, banki, c0mrade, Citi, Hacked!

Jegomość podpisujący się nickiem c0mrade chwali się na Pastebinie, że posiada dostęp do sieci wewnętrznej co najmniej 2 banków, w tym Citibanku i CoBanku. Jeśli chodzi o Citibank, c0mrade zdradza, że infiltrował go od 2008 roku...

4 lata na serwerach banku...

Na początek zastanówmy się co to znaczy dostęp do wewnętrznej sieci banku? Zaatakowanie komputera z którego korzysta jeden z pracowników? Root na bankowych serwerach? Wszystko wskazuje na to, że atakujący uzyskał dostęp do bankowych serwerów za pomocą udostępnianego przez bank oprogramowania, które (jak to w większości banków) jest obudowanym/okrojonym klientem FTP służącym do transferu raportów/kwitów/sprawozdań. Po wyciągnięciu danych z takiego klienta można próbować eskalacji przywilejów na serwerze FTP i najwyraźniej taką metodę ataku obrał c0mrade.

```
-----------
Logins:
-----------
karthik.b512@gmail.com:cobank:94[redacted]
Surya@gmail.com:N'Account:949[redacted]
```

c0mrade prezentuje część przechwyconych danych

c0mrade opublikował fragmenty przejętych przez siebie informacji, oraz wyjaśnił, że na serwerach banków przebywał kilka ładnych lat, czekając na odpowiedni moment. Intruz zdradził również, że oprócz Citibanku, przejeął kontrolę nad serwerami Cobanku, a jako dowód opublikował w internecie kod źródłowy wykorzystywanego przez bank oprogramowania.

Analiza udostępnionych przez c0merade'a danych wskazuje na to, że zaatakowany oddział Citibanku nie jest oddziałem polskim.