Gauss samples - Nation-state cyber-surveillance + Banking trojan

contagiodump.blogspot.com/2012/08/gauss-samples-nation-state-cyber.html

Just a quick post for those who can't sleep until get to play with Gauss

Here is a great paper by Kaspersky Gauss:Abnormal Distribution

and the blogpost: "Gauss: Nation-state cyber-surveillance meets banking Trojan"

Excerpt:

The highest number of infections is recorded in Lebanon, with more than 1600 computers affected. The Gauss code (winshell.ocx) contains direct commands to intercept data required to work with Lebanese banks – including the Bank of Beirut, Byblos Bank and Fransabank.

> In Israel and the Palestinian Territory, 750 incidents have been recorded." (Kaspersky)

Download

 Download all the files listed below as a password protected archive (email me if you need the password)

List of files

List of files for download:

```
├──devwiz.ocx
│       CBB982032AED60B133225A2715D94458_devwiz.ocx
│
├──dskapi.ocx
│       08D7DDB11E16B86544E0C3E677A60E10_100-dskapi.ocx
│       23D956C297C67D94F591FCB574D9325F_100-dskapi.ocx
│
├──mcdmn.ocx
│       9CA4A49135BCCDB09931CF0DBE25B5A9-mcdmn.ocx
│
├──smdk.ocx
│       5604A86CE596A239DD5B232AE32E02C6_smdk.ocx
│       90F5C45420C295C73067AF44028CE0DD_smdk.ocx
│
├──windig.ocx
│       DE2D0D6C340C75EB415F7263388351
25_windig.ocx
│
└──winshell.ocx
       4FB4D2EB303160C5F419CEC2E9F57850_winshell.ocx
       7AC2799B5337B4BE54E5D5B03B214572_winshell.ocx
       EF6451FDE3751F698B49C8D4975A58B5_winshell.ocx
```