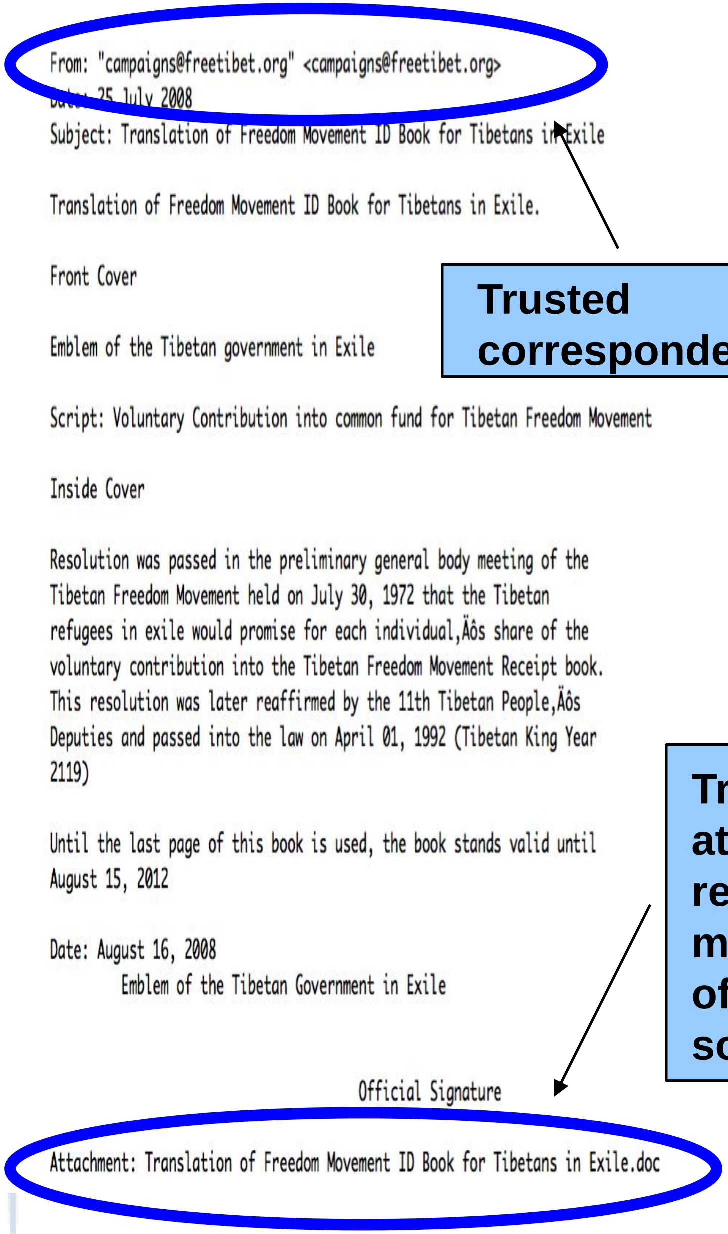
What We’re Up Against – Gh0stnet Example



From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the Tibetan Freedom Movement held on July 30, 1972 that the Tibetan refugees in exile would promise for each individual,Äôs share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People,Äôs Deputies and passed into the law on April 01, 1992 (Tibetan King Year 2119)

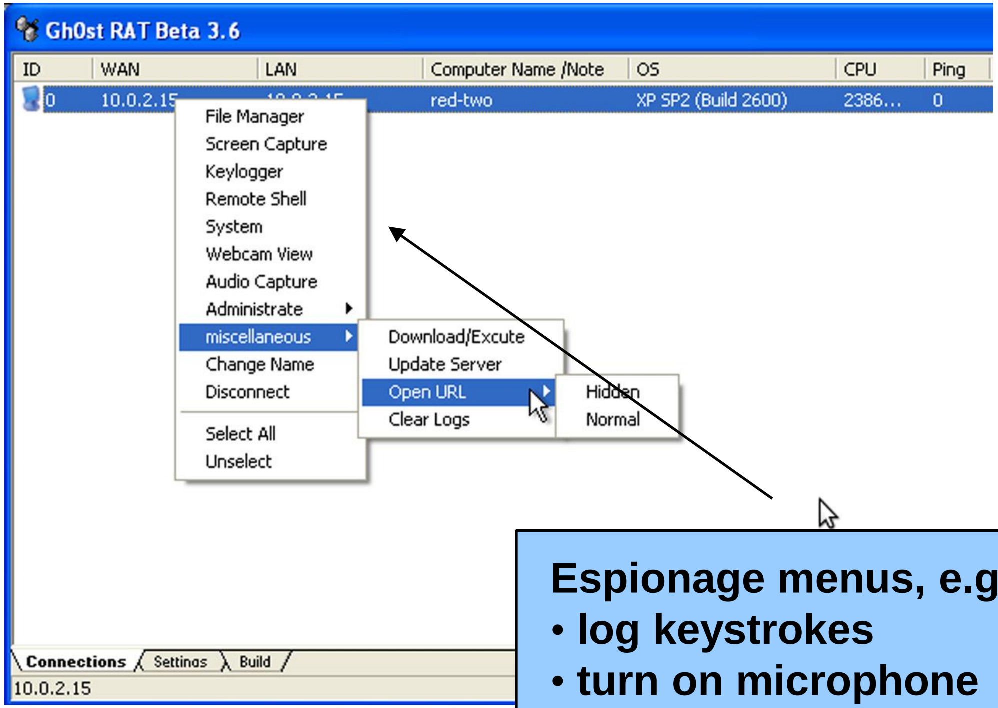
Until the last page of this book is used, the book stands valid until August 15, 2012

Date: August 16, 2008
Emblem of the Tibetan Government in Exile

Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc

Trusted correspondent



Gh0st RAT Beta 3.6

ID	WAN	LAN	Computer Name /Note	OS	CPU	Ping
0	10.0.2.15	10.0.2.15	red-two	XP SP2 (Build 2600)	2386...	0

Espionage menus, e.g.:
- log keystrokes
- turn on microphone
- turn on webcam

Trusted attachment, not recognized as malware by 2/3 of antivirus software

Who got burned? – a few examples:
- Tibet government in exile
- Numerous other governments / embassies (e.g. Germany, India, Iran, Korea, Indonesia, Pakistan, Bahrain)
- ASEAN, Asian Development Bank
- Petro Vietnam
- Associated Press

Nowhere to Hide

- "It's a Microsoft problem"
  - Apple and Linux far from immune
- "It's a password problem"
  - Real-time token compromises
- "We can verify transactions offline"
  - VOIP, Google Wave?
- "Air gaps protect essential networks"
  - Conficker and European military
- "I'm not that interesting"
  - $60 thousand in assets puts you in top 10% of global wealth
  - Mass customization of malware

- Limited regulatory solutions
  - Security standards / liability
  - Investment / procurement controls
- Moore's law favors the outlaws
- Longer term
  - Change Internet protocols
  - End to anonymity?