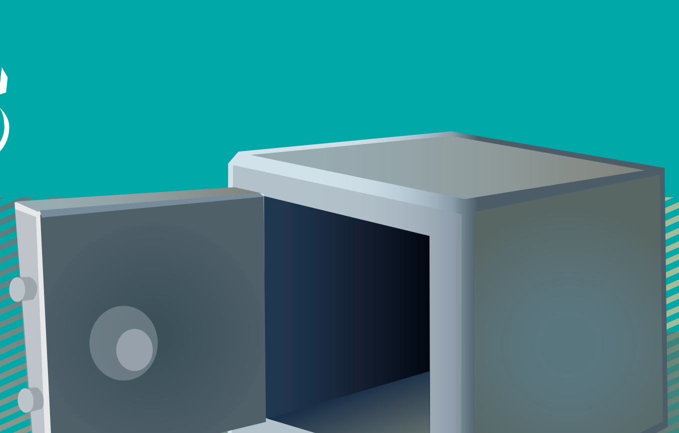
HOW to rob BANKS in the 21ST century?

HOW BANKING TROJAN ECOSYSTEM WORKS & FACTS ON ONLINE BANKING and CYBER THEFT



74 % of consumers do online banking

85 % are afraid of doing online banking via public PCs or via open wireless networks

35 % are not confident that their bank offers enough for safe banking

390 FBI cases of banking fraud as of 2010

Attempted loss by these acts: **$220,000,000**

Actual loss: **$70,000,000**

Sources: *http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud, F-Secure Broadband Survey, Spring 2012 **

5 STEPS TO ROB A BANK:

A STEP BY STEP BANKING TROJAN EXPLAINER

STEP 1

LOCATE THE AUDIENCE. THAT'S A JOB FOR **A SPAM GUY.**

E-mail! Why are we still using it?

E-mail spam is still one of the most effective ways to reach a wide audience. The task is accomplished by pros that target potential victims with authentic looking and well localized "invoices". The victim is baited into checking on a "canceled order" and the spammer's job is done.

STEP 2

LINK THE SPAM TO AN **"EXPLOIT KIT"**

Fortunately for bank robbers (and unfortunately for their victims), most people don't keep their web browsers and other installed software up to date. This means there's always plenty of known vulnerabilities to take advantage of which will give access to their computers. Exploit kits are easy to purchase on the web and there are numerous gangs selling exploit services.
If only people patched more than once a year! (Too bad for them that they don't.)

STEP 3

Exploits open the door-

IN WALKS A TROJAN DOWNLOADER

This is where the computer is "infected" with a guest that won't easily go away. The trojan downloader can then be used to pull down any number of additional threats, including banking trojans.

STEP 4

BANKING TROJAN

The banking trojan is installed, and the bank robbers get to work.
The spam, exploit, download part of the ecosystem has done its work! The infected computer is now under the control of a banking trojan gang which then monitors the computer for banking activity. Advanced banking trojans act in real time with "man-in-the-middle" attacks*. You think you're paying your bills but meanwhile, your money is going elsewhere.

STEP 5

How to get the cash out from the bank? Hire some

MONEY MULES

How to hire? Spam of course! The bait is typically a job offer for "money transfer agent" which is made out to be a legitimate job. The thieves claim to be a legit company which needs to outsource payroll, and then offers to transfer funds into the mule's account. The newly hired "employee" only needs to withdraw 90% of the funds and forward it on to the recipients (via an untraceable method, of course!). (Too bad for the mule when the bank investigators come knocking...)

**The F-Secure broadband survey covered web interviews of 6,400 broadband subscribers aged 20–60 years from 14 countries: France, the UK, Germany, Sweden, Finland, Italy, Spain, the Netherlands, Belgium, USA, Canada, Brazil, India and Japan. The survey was completed by GfK, 25 May–1 June 2012.*

Copyright ©2012 F-Secure Corporation

www.banking-protection.com

F-Secure