Council of Europe
Project on Cybercrime in Georgia

Romanian Experience

Tbilisi-13 May, 2010

ELECTRONIC FRAUDS

- Internet Fraud
- Credit Card Fraud
- Auction Fraud
- Phishing Attacks
- Wire Fraud
- Identity Theft

- **Phishing attacks**

Subjects are using different techniques to get access at customer information and than create fake web pages and send them messages which look like the messages from a real Bank or FI, etc

Subject are sending fake messages to different companies and attached a key logger in order to get access at the computer system and personal information of the customers

- **Targets**

-Bank accounts

-Credit card information

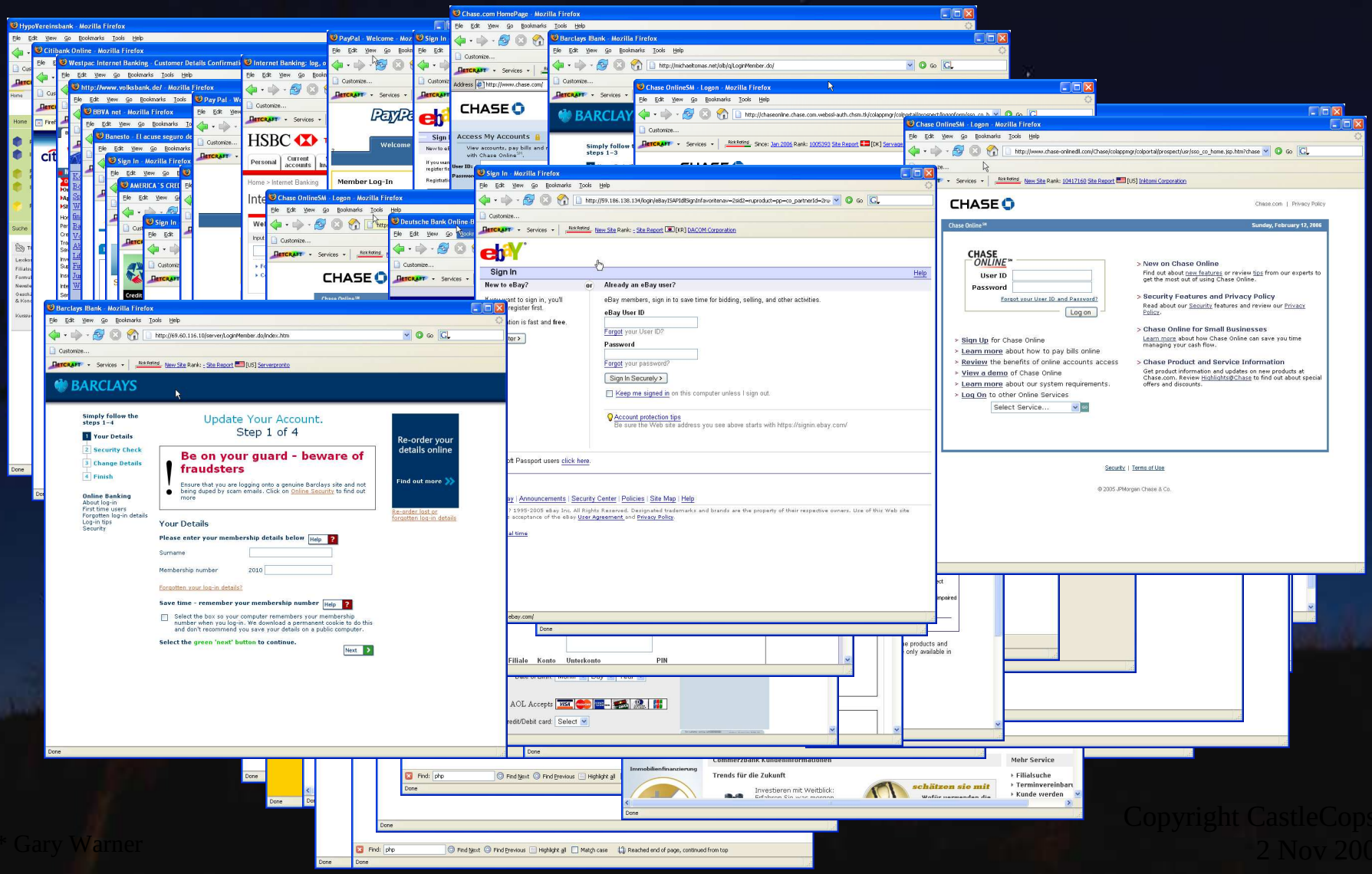
-Users information

- **Country hosting most phishing sites?**
  - United States (25%)
  - China (10%)

- **Countries hosting Trojan downloader's?**
  - China (46%)
  - United States (39%)

- **Most targeted Industry Sectors?**
  - Financial (93%)
  - Retail (2%)
  - ISP (3%)

Phishing Examples



* Gary Warner

2 Nov 2006

Romanian Phishing Attacks

March 2007

-RNP received a complaint from a RB regarding 5 phishing attacks against customers for credit card information

Facts:

-25 customers answered to the fake messages
-6 victims, the losses 100.000 RON
-fraudulent withdrawals from ATMs in Constanta and Bucharest
- period March-May 2007 –totally 15 phishing attacks
-fake site-s hosted in US,
-no subjects information
-no IP,s or email accounts from Romania
-no images from ATM-s video system

Investigations:
-close cooperation with the Bank representatives
-monitoring all the new phishing sites
-statements from victims and important information about phishing sites and fake messages
-analyzing the phishing sites
-monitoring the credit card transactions
-subpoena for Yahoo through a MLAR sent to US Authorities
-surveillance
-monitoring Internet connections and phone conversations

Results:
- 2 IP,s from Romania used to download the site-s and connect to the drop boxes
-one address from Bucharest and one person from Constanta
-skimming devices installed on Brasov –June 2007
-skimming devices installed on Constanta –October 2007

Criminal activities:

-phishing attacks against RB
-ATM frauds
-Phishing attacks against US Banks
-WU frauds

November 2007

-23 search warrants were conducted
-18 people were charged
-11 people were arrested
-computer, skimming devices, blank cards, etc were seized

I

2006 February 23rd

- DIOCT receives information regarding fraudulent withdrawals from ATMs in Constanta and Bucharest
- Dynamic surveillance was set

Results:

- a small organized group, very cautious, using fast cars and deceiving maneuvers for entrapping possible surveillance, determined jobs set for it's members (one stayed in the car with the face covered, at least two were supervising the premises, other two were using some counterfeited cards for withdrawals
- after the facts meeting was set with the leader

People involved identified in the 23rd operation

Leader CG

Lieutenants

MC

On 24TH the operation continued with the same modus operandi.

Based on the surveillance material were tracked the ATMs used (some cards were captured and recuperated by the police) and from the credit card processors were listed the fraudulent transactions

Total amount 600 mil.lei (cca.16.900 Euro)

The cards were originally issued by Italian Banks

From local intelligence we've learned that the fraudulent activity in Constanta was conducted by CG and one of his lieutenants COL

- CG was also known as the G**odfather** for several people near to him including for MC (because of his role in the weeding services as spiritual father of the newly weds)
- CG was as well known as a businessmen, owner of a few companies along with one of his godsons MC.

Intelligence revealed as well close cooperation between CG and MI, who was operating in Bucharest.

One of his lieutenants was identified as his natural son

MG

Members of MI' subgroup

DCC SE IC LC

On February 27Th the court issued orders for communication interceptions / phones/emails

The orders were extended for a period of 4 months, which is the maximum allowed by the Romanian Penal Procedural Code

- Results:

  - **Preparing, planning and financing** operating teams known as well as squads or brigades for Italy, Spain, Sweden, Denmark) in order to install on POS units and afterwards to retrieve manufactured electronic devices able to collect sensitive information related to electronic instruments used for payments

  - Financing the manufacture of the devices

  - Collecting information related to different types of POS or ATMs

  - Balance benefits/costs/losses

  - Modus operandi – simulated burglaries for covering the real target : installing the electronic devices

    - cooperation with employees

  - The layers/ chain of command and execution

- **Other people identified, subgroup, in relation with both chain of command CG and MI:**

BC

AF

Results from wire tapping:

- conversations about brigades decimated by LE from Sweden, Denmark and Italy
- AF escaped from Sweden and than from Denmark
- COL, aka Shorty was the coordinator of CG's squads in Italy and Spain
- one of Bucharest leader' squad arrested on May 27Th in Italy, Torino

Information exchanged with Sweden showed only collateral links with the Romanian leaders CG, MI

The Romanian Liaison officer couldn't establish the real location of the arrested people in Torino

The take down : June 27th

23 Simultaneous search warrants issued and served in Constanta and Bucharest

6 arrested including the leaders CG and MI along with 4 of their lieutenants

8 arrest warrants in absentia were issued for the other members of the group including COL and other members (no international warrants was requested then, nor extradition)

Other members were charged but not arrested

- **Results of house searches:**

  - computers
  - manufactured devices (ATM' keyboard and front)
  - plastics

- **Results of computer searches:**

  - email correspondence matching with the material intercepted
  - images of ATMs, models, other devices examples of how to manufacture
  - software for writing the magnetic band of a credit card, drivers for other devices

- The defendants didn't cooperate with the police officers nor with the prosecutor

10.10.2006

The indictment was issued for 7 defendants :

Charges : initiating and constituting of an organized group with the purpose of committing aggravated crimes, forgery of credit cards, unlawful use of credit cards information, fraudulent operations with credit cards, manufacturing and possession of devices in order to forge/counterfeit credit cards.

Penalty : imprisonment from 3 to 15 years

QUESTIONS ?