Cyber Security Challenges in the Financial Sector:
Internal and External Threats
Cyber Security Challenges in the Financial Sector: Internal and External Threats
Agenda

- About...
- Why do we have to be worried?
- First story: The crazy cash machine
- Second story: Cyber Bonnie and Clyde
- Conclusions
- Questions & answers
- Contact information
About...

What is Mnemo?
- Founded in 2009
- Presence in 2 Spanish companies
- Headquarters in Madrid, Spain
- More than 1,100 employees
- Operations in 14 countries
- Including services in Colombia, France, and Spain
- Annual sales totaling $100 million
- Among the 100 largest companies in the following sectors:
  - Public sector
  - Defense
  - Finance
  - Industry
  - Oil & Gas

Goals
- Taking about the offer of the information security services for the private sector
- Taking you stories from real work situations
- Making aware the need for crisis communication and more information security
- Making aware everybody about them topics: information security, crisis communication, and more information security.
What is Mnemo?

- Founded in 2000
- Privately held Spanish company
- Headquarters in Madrid, Spain
- More than 1,000 employees
- Operations in twelve countries including Mexico, Colombia and Saudi Arabia
- Annual sales totaling 100 million dollars.
- More than 100 customers of the following sectors:
  - Public Utilities
  - Government
  - Finance & Banking
  - Industry
  - Oil & Gas
Goals

- Talking about the danger of the information security incidents for the private sector.
- Talking you stories from real world not from surveys or estimations
- Making aware everybody about deep incidents investigation and more information control
Why do we have to be worried?

Financial Data Breaches in the last years

Small Analysis
Financial Data Breaches in the last years

**RAK BANK**
- Organization: Rak Bank
- Country: 20 countries
- Type of Breach: The scammers made 4,500 ATM transactions
- Time: December 2012 to Feb 2013
- Extend of loss: $5 million in total. Just in New York, they made 750 fraudulent transactions and stole $400,000 from 140 ATMs

**Bank Muscat**
- Organization: Bank of Muscat
- Country: 24 countries
- Type of Breach: Using card data from the Bank of Muscat, cells in 24 countries
- Time: December 2012 to Feb 2013
- Extend of loss: $15 million. Hackers made 36,000 transactions over 10 hours. In New York, they got $2.4 million from 3,000 ATMs in the city

**Michaels**
- Organization: Michaels
- Country: USA
- Type of Breach: PoS / Data leakage (Cards)
- Time: May 2013 to January 2014
- Extend of loss: Approximately 2.6 million cards

**Neiman Marcus**
- Organization: Neiman Marcus
- Country: USA
- Type of Breach: Data leakage (Cards)
- Software (malware) was installed on their system
- Time: July - October 2013
- Extend of loss: It affected a maximum of 350,000 customers. 1.1 million credit and debit cards

**P.F. Chang's**
- Organization: P.F. Chang's China Bistro
- Country: USA
- Type of Breach: Credit- and debit-card-processing system
- Extend of loss: Stolen records were being sold for between $18 to $140 per card, the price depending on how fresh the stolen data is

**HSBC**
- Organization: HSBC
- Country: Turkey
- Type of Breach: Data leakage (Cards)
- Time: November 2013
- Extend of loss: 2.7 million credit cards exposed

**Affinity Gaming**
- Organization: 11 casinos under Affinity Gaming
- Country: USA
- Type of Breach: Data leakage (Cards)
- Time: December 2013 to April 2014
- Extend of loss: Customer information of the clients who acquired Non-gaming purchases like resorts and other services

**JPMorgan Chase**
- Organization: JPMorgan Chase
- Country: USA
- Type of Breach: Data theft (names, emails, contact numbers and addresses)
- Time: July 2014
- Extend of loss: 76 million households and 7 million small businesses

**The Home Depot**
- Organization: Home Depot
- Country: USA & Canada
- Type of Breach: PoS / Data leakage (cards)
- Time: Sep - Nov 2014
- Extend of loss: 56 million credit and debit cards and 53 million email addresses

**Target**
- Organization: Target
- Country: USA
- Type of Breach: PoS / Data leakage (cards)
- Time: November 2013
- Extend of loss: $110 million of personal and financial records and $248 million of dollars

**AllCrypt**
- Organization: AllCrypt
- Country: Unknown
- Type of Breach: Used an exploit in WordPress to breach the security
- Time: March 2015
- Extend of loss: 42 Bitcoins stolen by the hackers
Organization: HSBC
Country: Turkey
Type of Breach: Data leakage (Cards)
Time: November 2013
Extent of loss: 2.7 million credit cards exposed
Organization: JP Morgan Chase
Country: **USA**
Type of Breach: **Data theft (names, emails, contact numbers and addresses)**
Time: **July 2014**
Extent of loss: **76 million households and 7 million small businesses**
Small Analysis

This chain of supermarkets had a good run at the New York Stock Exchange in late 2013.

Was it because of January?

In January 2014, it was unveiled that the financial information of 110 million customers of Target had been compromised, the company’s shares plummeted.

I wish it was only January

Throughout 2014, Target could not raise the value of their shares significantly, they had to spend a whole year to observe a remarkable recovery.
This chain of supermarkets had a good run at the New York Stock Exchange in late 2013.
Was it because of January?

In January 2014, when it was unveiled that the financial information of 110 million customers of Target had been compromised, the company's shares plummeted.
Throughout 2014, Target could not raise the value of their shares significantly, they had to spend a whole year to observe a remarkable recovery.
First story: The crazy cash machine

Starring: (cyber-evil) etc.
- Money mule
- Investigator
- George (Inside)
- Head of Fraud Management
- Bandit (ATM)

Facts:
- Phishing is the easiest way for criminals to install malware
- Early versions of Pulsus allow the attacker to remotely control the machine
- The latest version phases a remote connection

Actions:
- Pulsus can be downloaded from the web
- About 50% of ATMs are still using Windows XP

Conclusions:
- Microsoft finished regular support for Windows XP on April 8, 2014
- About 50% of ATMs are still using Windows XP
- Phishing is the easiest way for criminals to install malware
- Early versions of Pulsus allow the attacker to remotely control the machine
- The latest version phases a remote connection

Starring

(Cyber-maloso)
Hacker

Money mule

George
(Insider)

Head of Fraud Management

Investigator

Bank (ATM)
**Facts**

**Fact 1**
- He obtained money without using a card.
- A victim's machine was compromised by malware from an ATM.

**Fact 2**
- Cyber-attacker installs malware through a CD-ROM.
- Cassette contains the data of the ATM.

**Fact 3**
- Fraud management department receives a security alert and looks at security cameras.
- Head of Fraud Management reviews the CD and starts an investigation.
Fact 1

A money mule withdrew money from an ATM.

He obtained money without using a card.
Fact 2

Cyber-maloso develops or gets a malware focus on ATM and he meets George.

Cyber-maloso installs the malware through a CD-ROM.

George who holds the keys of the ATM leaves the ATM's door open.
Fact 3

Fraud management department received a security alert and looked at security cameras.

Head of Fraud Management collects the CD and starts an investigation.
Actions

Action 1
Bank requested Memento's expertise to perform a new investigation by using Malware Analysis Lab.

Action 2: Static analysis
Memento's Analyst
Static analysis showed the following results:

Action 3: Dynamic analysis
Dynamic analysis revealed the following findings:
Bank requested Mnemo's experts to perform a deep investigation by using Malware Analysis Lab.

Bank started an internal investigation to collect all the useful information to clarify the security incident.

Head of Fraud Management gives the CD-ROM for analysis.
Action 2: Static analysis

Mnemo's Analyst

Static analysis showed up the following results:

**Finding 1**
- Phishing email contains a network service or executable file.
- The file opens in a portable executable.
- It is run with a command line argument.
- The file contains a data file.

**Finding 2**
- The file is a portable executable.
- It is run with a command line argument.
- The file contains a data file.

**Finding 3**
- The file is a portable executable.
- It is run with a command line argument.
- The file contains a data file.

**Finding 4**
- The file is a portable executable.
- It is run with a command line argument.
- The file contains a data file.
Finding 1

Ploutus is installed by inserting a CD boot disk which includes a `start.bat` file that does the following:

- Identify the CD drive and the file system directory
- Create NCRDRVPS registry key to install PloutusService.exe
- Copy several libraries (APTRA) and ploutusservice.exe file to Windows directory
Ploutusservice.exe file is a portable executable 32 .NET assembly and it is obfuscated with Confuser v1.9.0.0 which is an anti-debugger and encrypts codes.
Finding 3

- The key sequence to launch the application is F8 F1 F7 F3 F4 F2 F8.
- The malware requires an activation code that is generated based on the day, month and a random four-digit number which is stored in C:\Windows\Config.ini file after pressing F1 key.
- If the activation code is correct and the vendor is identified, the thief can dispense the money with F3 key. This activation code is valid for 24 hours.
- All the activities are recorded in C:\Windows\System32\log.txt file.
public class Keyboard
{
    public static void Read(int Data)
    {
    }

    public static void StartTheThread(int KeyData)
    {
    }

    private static void RealStart(int KeyData)
    {
    }

    private static void RealStart(KeyEventArgs KeyData)
    {
        if (KeyData.KeyCode == Keys.F8)
        {
            if (MemoryData.Command == "F8F1F7F3F5F4F2")
                Program.NCRV.UIEnable();
            MemoryData.Command = string.Empty;
        }
        if (MemoryDataGuiEnable)
        {
            if (KeyData.KeyCode == Keys.F1)
                Keyboard.ProcessCommandGui(1);
        }
    }
}
Finding 4

The procedure for generating the correct activation code is as follows:

1. Press F1 key to generate a random number.
2. Look for the random number stored in the C:\Windows\Config.ini file (DATAAA)
3. Get the system date
4. Use the CryptTrack algorithm located in CryptClass, passing as inputs previous obtained values.
5. Use AddCero function to generate a string of 8 digits and select the activation code on the app.
6. Press F2 key to active the ATM, and the generated code should be working!!!
else if (CMD == 2)
{
    Util.UpdateLog("Activate");
    if (MemoryData.ActivatedID == Util.AddCero(CryptClass.CryptTrack(now.Day, now.Month, int.Parse(s)).ToString()))
    {
        TimeSpan span = (TimeSpan) (DateTime.UtcNow - new DateTime(0x7b2, 1, 1, 0, 0, 0));
        IniFile.IniWriteValue("Config", "DATAC", CryptClass.GetMd5Hash(MemoryData.ActivatedID));
        Program.NCRV.UpdateText("ATM: OK DATE: " + DateTime.Now);
        Util.UpdateLog("ACTIVATE OK");
    }
    else
    {
        Program.NCRV.UpdateText("ATM: ALREADY ACTIVE DATE: " + DateTime.Now);
        Util.UpdateLog("ACTIVATE ALREADY");
    }
}
else
{
    Program.NCRV.UpdateText("ATM: INVALID ACTIVATION CODE DATE: " + DateTime.Now);
    Util.UpdateLog("ACTIVATE INVALID");
}
Action 3: Dynamic analysis

Installation

* Plutus is installed by inserting a bootable Windows CD-ROM from the original Windows XP that means you need physical access.

Execution

We executed a key sequence F4, F1, F7, F3, F4, F2, F8, which was obtained during code analysis, to initiate the malicious application.

* GUI can be manipulated using keyboard with the following keys:
  - F1: Generate ID
  - F2: Active ATM
  - F3: ID key
  - F4: Dispen
  - F5: Login key
  - F7: Right key
  - F8: Left key
Installation

- Ploutus is installed by inserting a bootable Windows CD-ROM from the original Windows XP that means you need physical access.

Execution

- We executed a key sequence F8 F1 F7 F3 F4 F2 F8, which was obtained during code analysis, to initiate the malicious application.

GUI can be manipulated using keyboard with the following keys:
- F1: Generate ID
- F2: Active ATM
- F3: Dispenser
- F4: Disable GUI
- F5: Up key
- F6: Down key
- F7: Right key
- F8: Left key
Installation

- Ploutus is installed by inserting a bootable Windows CD-ROM from the original Windows XP that means you need physical access.
Execution

We executed a key sequence **F8 F1 F7 F3 F4 F2 F8**, which was obtained during code analysis, to initiate the malicious application.

GUI can be manipulated using keyboard with the following keys:
- **F1**: Generate ID
- **F2**: Active ATM
- **F3**: Dispenser
- **F4**: Disable GUI
- **F5**: Up key
- **F6**: Down key
- **F7**: Right key
- **F8**: Left key
**Activation code**

```csharp
If (MemoryData.ActivatedID ==
    Utils.AddCero(CryptClass.CryptTrack(now.
    Day, now.Month, int.Parse(s)).ToString()))
```

**Random number**

```
ATM ID: 5482
```

**Successful activation**

```
ATM OK DATE: 15/10/2013 3:15:10 PM
Dispense Receive
Dispense Bill: 40 Count: 3
DISPENSE START BILL: 40 DATE: 15/10/2013 3:15:29 PM
Vendor Init OK
Vendor Mode: XFSAVAILABLE
System Mode: VDMNORMAL
vdm_AvailabilityChanged:15/10/2013 3:15:30 PM Status: XFSAVAILABLE
vdm_EntryRequested:15/10/2013 3:15:30 PM
```
Conclusions

- Ploutus isn't the easiest piece of malware to install, as cybercriminals need to have physical access to the machine.

- Early versions of Ploutus allowed to be controlled via the numerical interface on an ATM or by an attached keyboard. But the latest version shows a remarkable new development: it is now controllable remotely via text message.

- About 95% of ATMs are still running Windows XP. Microsoft finished regular support for Windows XP on April 8 last year, but is offering extended support for Windows XP embedded systems, used for point-of-sale devices and ATMs, through January 2016.
Second story: Cyber Bonnie and Clyde

- **Starring**
  - Cyber-Bonnie
  - Cyber-Clyde
  - Anna Chief
  - Bank
  - Investigator

- **Facts**

- **Actions**

- **Conclusions**
  - It is really worrying and disturbing that some of them are still involved with phishing domains, because this fact could mean that cyber criminals are now getting into the institutions and that they are starting to work with more intelligence and organization.
  - Due to the lack of well-implemented on-premises security policies, the bank could not have this case to the court, despite the good practice that means. Focusing on presence and digital evidence and the results of the investigation.
Starring

Cyber-Bonnie

Cyber-Clyde

Area Chief

Investigator

Bank
Fact 1:
Area Chief gave the bank's systems administrator access to all restricted areas.
Customer service reports were modified to hide suspicious transactions.

Fact 2:
The information was in the computer database.
Chloe saw the information on a computer monitor.

Fact 3:
Bank's fraud investigation department was led by the chief to the area where the Area Chief and Bonnie worked.

The estimated amount of stolen money is around USD 500,000. 25% of this goes for Bonnie and Chloe.
Fact 1

Area Chief gave his Bank's system credentials to Bonnie in an unauthorized way.

Bonnie, an internal worker of the Bank uses the Chief's credentials to apply daily operations and also she set fraudulent changes.

Many customer accounts records were modified in the Bank's systems by Cyber-Bonnie.
Fact 2

Bonnie got the information of the fraudulent modified accounts and she sent it to an external email account.

The information was in the email body and attached as spreadsheet format as well.

Clyde used the information to get a limited amount of cash from Bank's ATMs without a card by taking advantage of a service of the Bank for mobile devices.
Fact 3

Bank realized the fraudulent behavior and a large amount of money withdrawn and then started to track the operations according to the patterns.

Bank's fraud investigation department was lead by the clues to the area where the Area Chief and Bonnie worked.

The estimated amount of stolen money is around 500,000 USD only for Bonnie and Clyde.
Actions

**Action 1**
- Bank requested MEMO experts to perform a deep investigation by usingignant measures and Cyber-intelligence techniques.
- The investigation involved the recovery of forensic images of the involved computers and online accounts to obtain relevant information.

**Action 2: Digital Forensics**
- Memory investigation was conducted.
- An attacker's computer was examined.
- Digital forensic analysis revealed the following:
  - Exchanges of information of the affected accounts
  - Evidence of mass mailing to the external users
  - Evidence of mass mailing to the affected accounts
  - Evidence of the use of USB devices on internal and external computers
  - Both computers had malware accounts installed and used by attackers
- The results helped in the recovery of important data for the investigation.

**Action 3: Cyber-Intelligence**
- Cyber-intelligence was used to analyze the data.
- The analysis revealed the following:
  - The external user's email address was compromised, leading to multiple accounts.
  - Malware was used by attackers.
  - Attacks were directed towards social networks and popular websites.

**MEMO**
- The MEMO team was involved in the investigation process.

---

For more detailed analysis and investigation, please refer to the attached report.
Bank requested Mnemo's experts to perform a deep investigation by using Digital Forensics and Cyber-Intelligence techniques.

First step was taking the forensic images of the involved computers and collect all the relevant information to obtain the case context.

Bank started an internal investigation to collect all the useful information to clarify the fraudulent facts.
Digital Forensic analysis show up the following results:

- Excel files with information of the affected accounts
- Remains of web emails to the external Clyde's email address
- Evidence of massive use of USB storage devices on Bank's computers
- Both computers had many users accounts including the Area Chief and Bonnie ones, there was for more users, as well
Action 3: Cyber-Intelligence

- Cyber-Intelligence findings resulted quite interesting, because the external Clyde's email address was involved with many Phishing Domains, some active and others disabled.
- Besides, Clyde’s and Bonnie’s Facebook profiles were found for both and we realized they were very related, they were spouses.
Conclusions

- It is really worrying and disturbing that one of them was related with Phishing Domains, because this fact could mean that cyber criminals are now getting into the institutions and that they are starting to work with more knowledge and organization.

- Due to the lack of well implemented internal security policies, the Bank could not take this case to the court, despite the good practices that Mnemo followed to preserve the digital evidence and the results of the investigation.
Conclusions

Continuing challenges

- Cybercriminals are inside organizations.
- Organizations are not prepared to handle this type of security incidents.
- They failed by not having appropriate protocols for the new type of probe new ways of attacks, and cybergangs.

Advice based on experience

- Don't work alone.
- Address the problem through a global approach.
- Start with a simple-to-complex tasks.
- Be more aware of the growing cybersecurity threats.
- Monitor the evolution of existing and emerging technologies.
- Take advantage of the information-sharing resources available.

To finish...

- Cybercrime is global. It has no borders or time zones... we have to face it with a different approach.
- Organizations need to:
  - change their structures
  - quickly respond to new types of crimes
  - create a position as head of intelligence, risk assessment officer
  - collaborate with others CERTs
Continuing challenges

- Cybercriminals are inside organizations.
- Organizations are not prepared to handle this type of security incidents.
- They failed by not having appropriate protocols for the new type of probe new ways of attacks, and cybergangs.
Advice based on experience

- Don't work alone.
- Address the problem through a global approach.
- Start with a simple-to-complex tasks.
- Be more aware of the growing cybersecurity threats.
- Monitor the evolution of existing and emerging technologies.
- Take advantage of the information-sharing resources available.
To finish...

- Cybercrime is global, it has no borders or timezones... we have to face it with a different approach.

- Organizations need to:
  - change their structures
  - quickly responde to new types of crimes
  - create a position as head of intelligence, risk assessment officer
  - collaborate with others CERTs
Contact Information

Rosa Xochitl Sarabia Bautista
Director of Mnemo-CERT
rx.sarabia@mnemo.com

Mnemo Evolution & Integration Services
www.mnemo.com
cert.mnemo.com
For not being like this...
Cyber Security Challenges in the Financial Sector:
Internal and External Threats