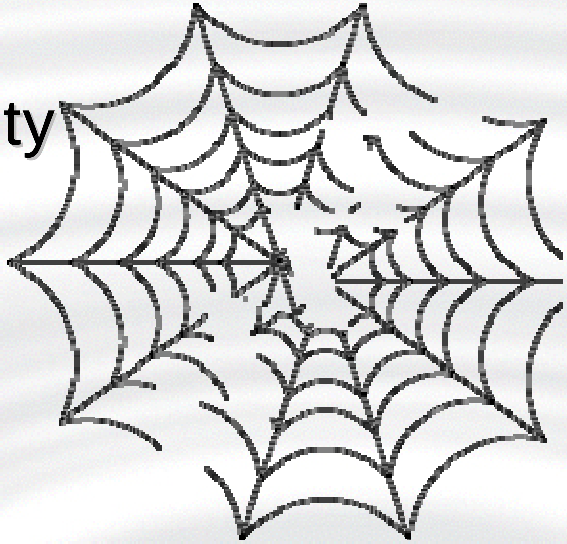
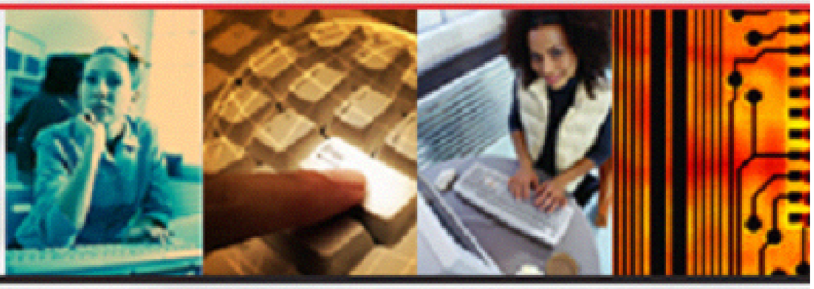
The Broken Web:

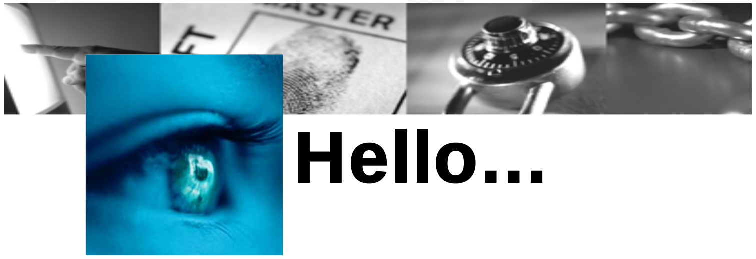
Identifying Weaknesses and Strengthening Internet Security



Steve Antoniewicz

02/19/2009





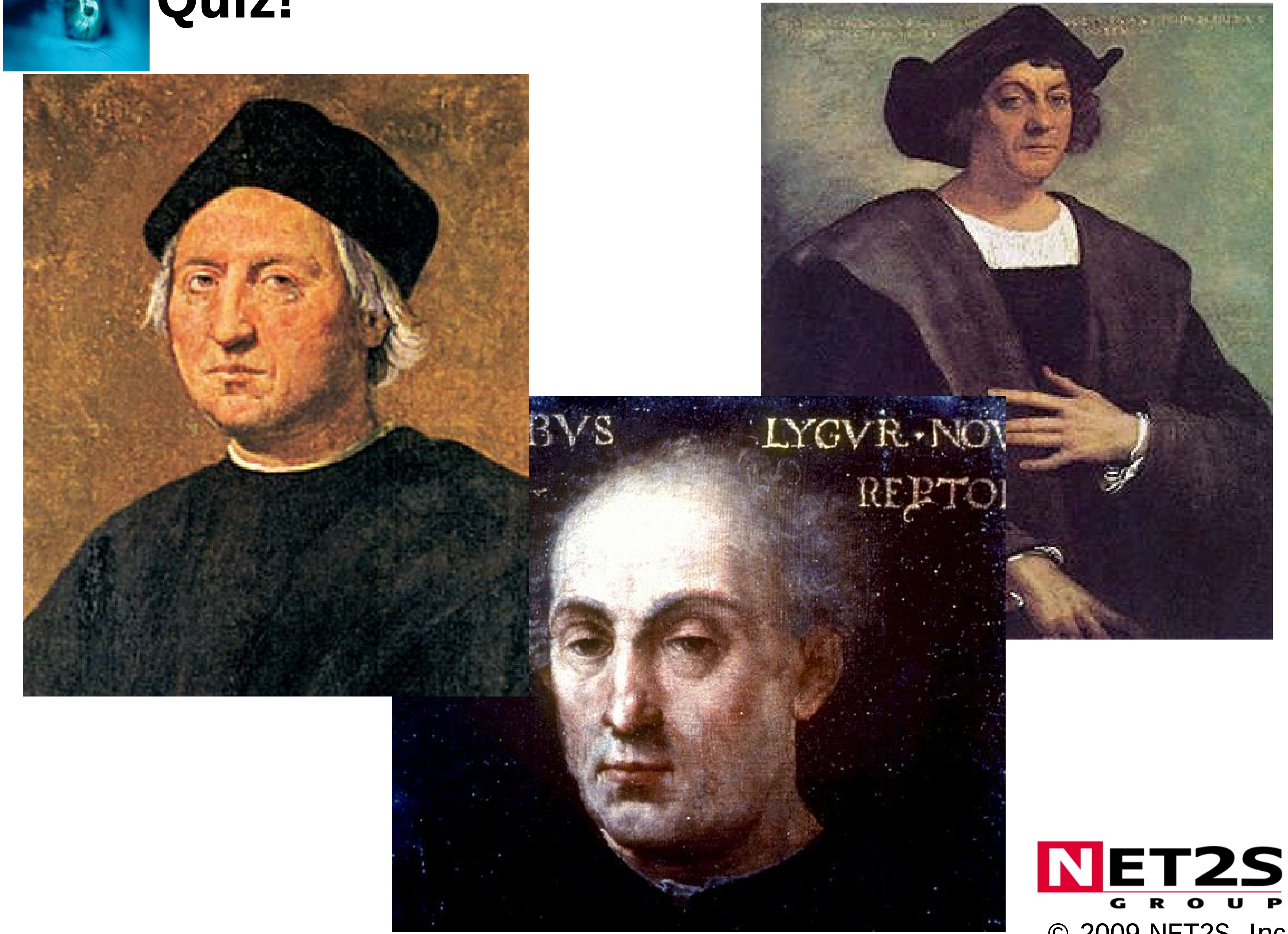
Hello...

- **I am:**
  - Steve Antoniewicz
  - Security Researcher
  - Technologist
  - Certified in a bunch of stuff
  - Employed by
    - NET2S / British Telecom

- **We are going to talk about:**
  - Crime
  - Hackers
  - The Internet

NET2S
GROUP

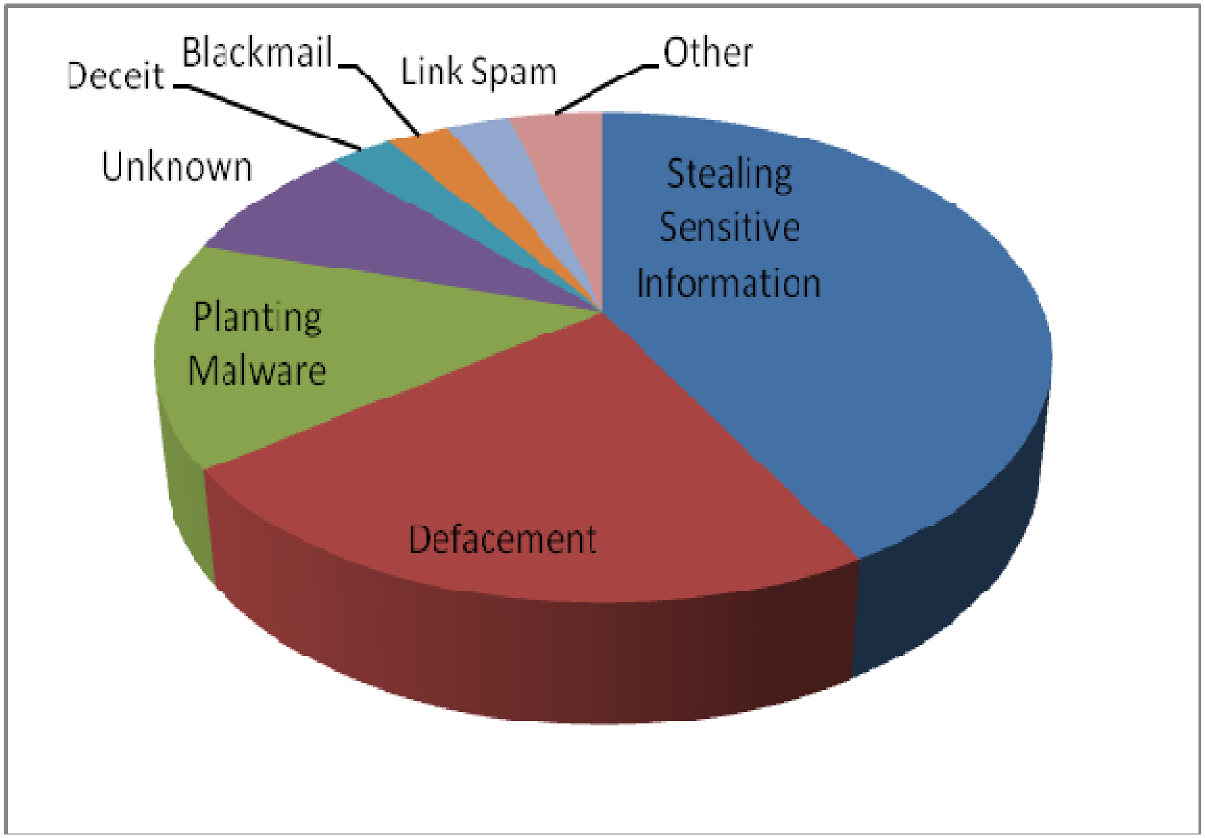
Quiz!



NET2S GROUP

Motivators

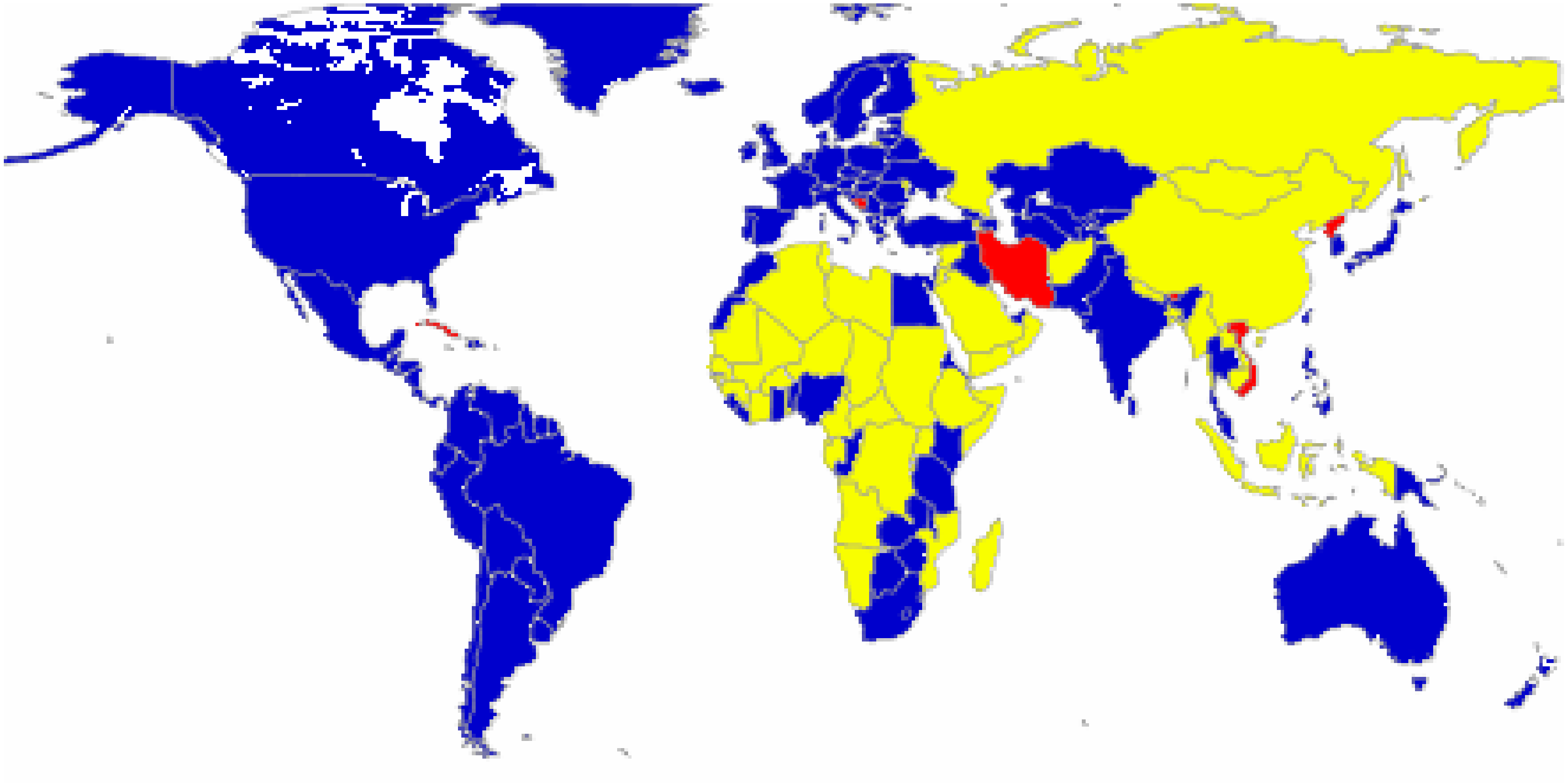
Disclosed Incidents



** Source: http://www.xiom.com/whid*

Evasion Techniques

- Foreign-hosted servers



🟨 Countries which the U.S. maintains diplomatic relations, but does not have extradition treaties with

🟥 Countries which have neither diplomatic relations nor extradition treaties with the U.S.

NET2S GROUP

Evasion Techniques

- Compromised hosts

- Open WiFi
  - Public Networks
  - Home / Corporate Networks

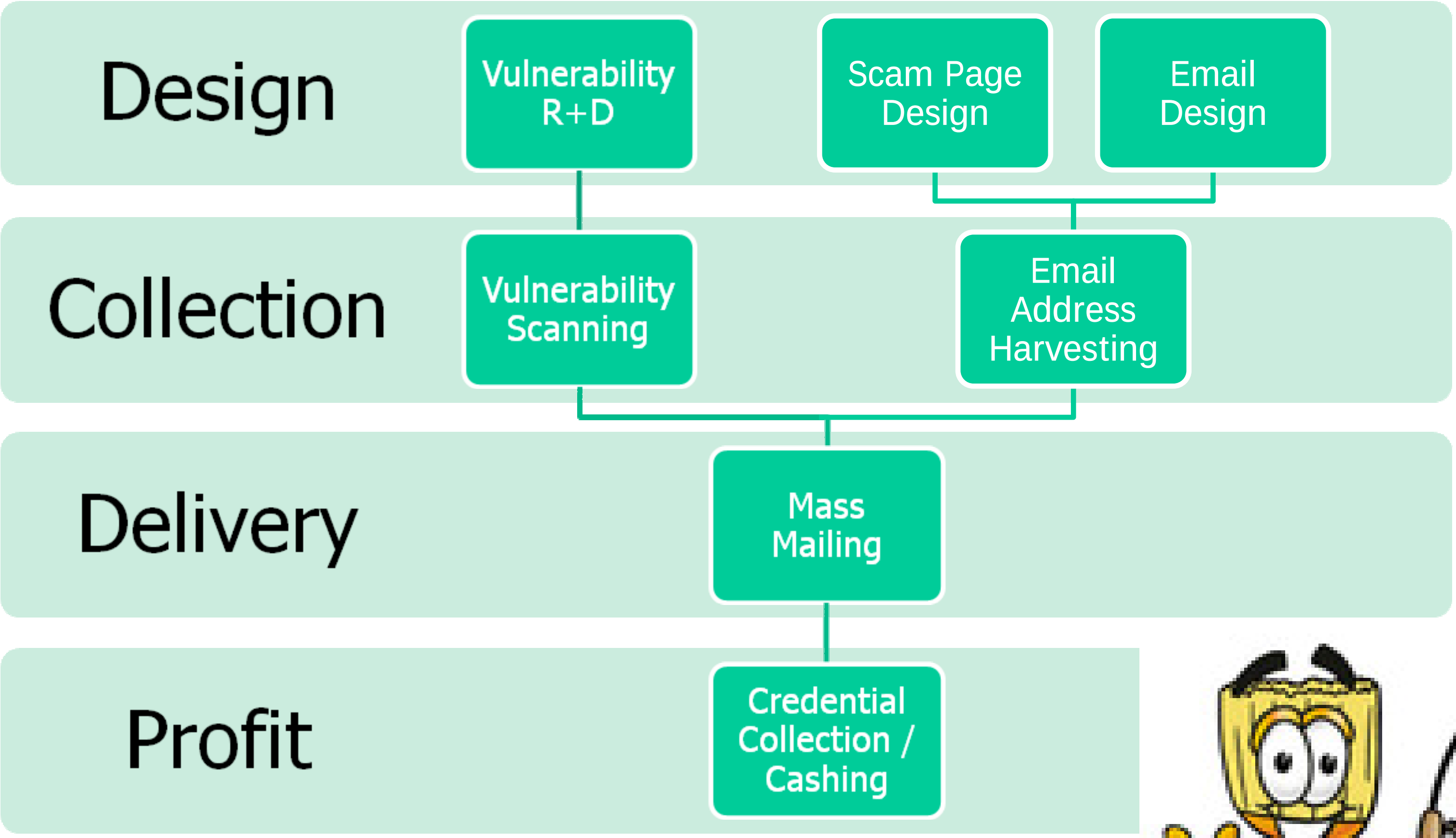
Phishing

- **Goals**
  - Monetary Theft
  - Identity Theft

- **2007 – $3.2 Billion Lost**
  - 3.6 Million adults in the US

** Source Gartner*

Phishing



Design

Vulnerability R+D

Scam Page Design

Email Design

Collection

Vulnerability Scanning

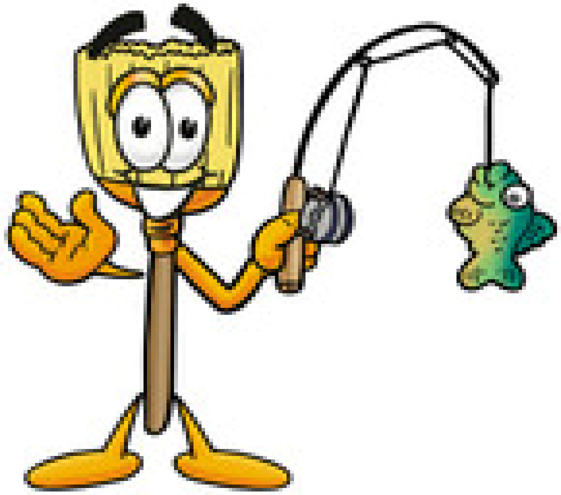
Email Address Harvesting

Delivery

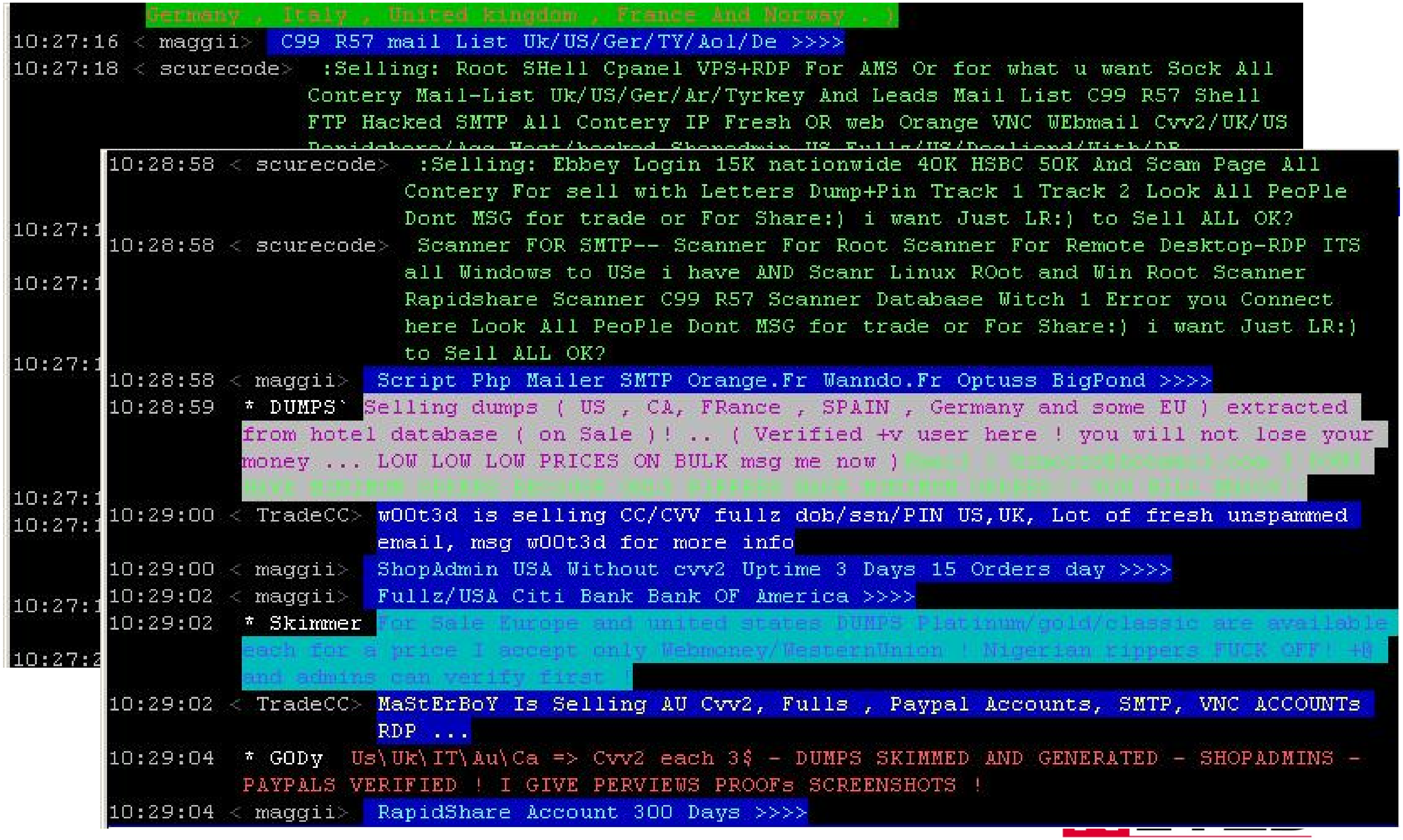
Mass Mailing

Profit

Credential Collection / Cashing



Phishing



```
         Germany , Italy , United kingdom , France And Norway . )
10:27:16 < maggii>  C99 R57 mail List Uk/US/Ger/TY/Aol/De >>>>
10:27:18 < scurecode>  :Selling: Root SHell Cpanel VPS+RDP For AMS Or for what u want Sock All
                       Contery Mail-List Uk/US/Ger/Ar/Tyrkey And Leads Mail List C99 R57 Shell
                       FTP Hacked SMTP All Contery IP Fresh OR web Orange VNC WEbmail Cvv2/UK/US
10:27:1
10:27:1
10:27:1
10:27:1
10:27:1
10:27:1
10:27:2
```

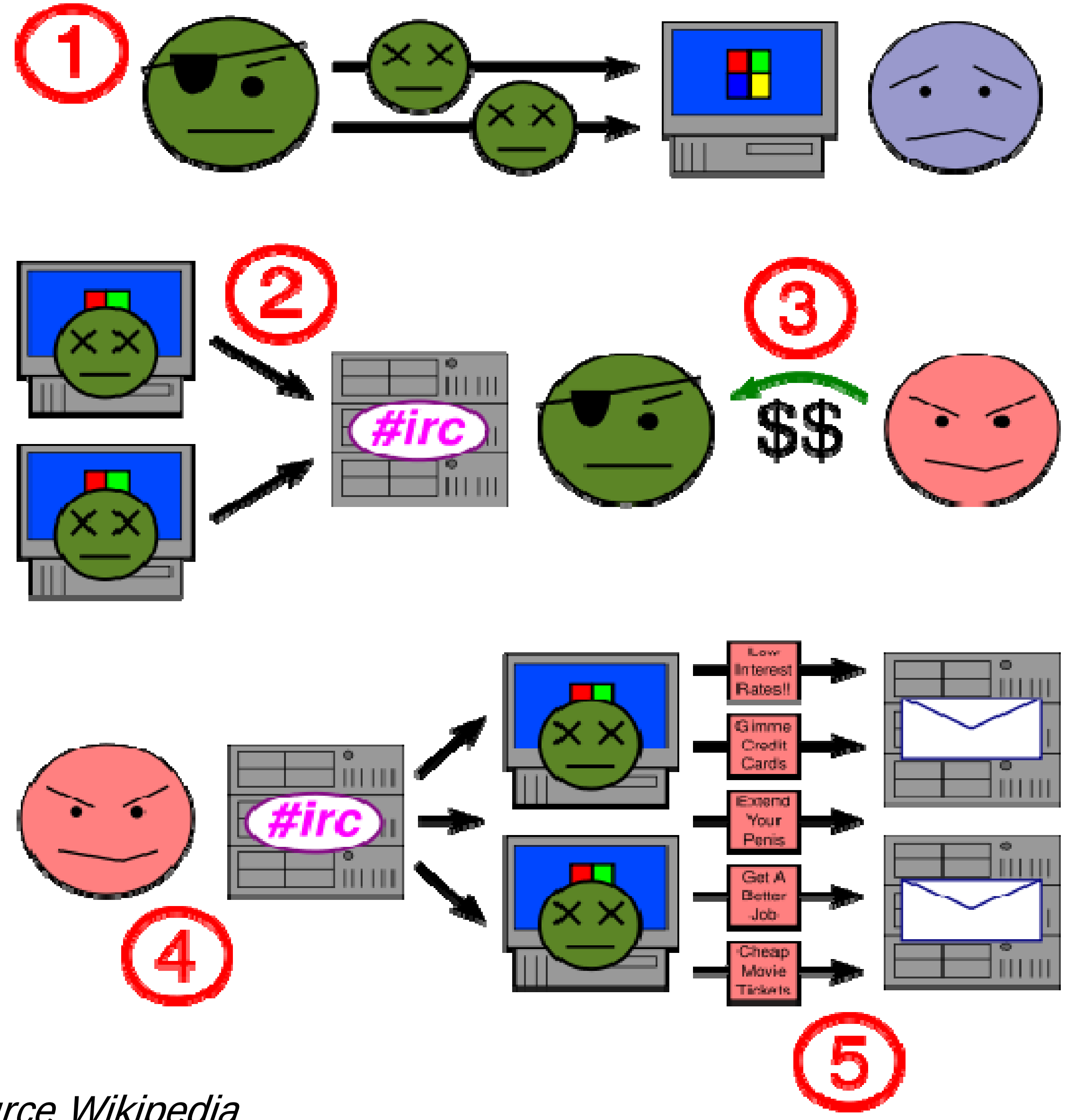
```
10:28:58 < scurecode>  :Selling: Ebbey Login 15K nationwide 40K HSBC 50K And Scam Page All
                       Contery For sell with Letters Dump+Pin Track 1 Track 2 Look All PeoPle
                       Dont MSG for trade or For Share:) i want Just LR:) to Sell ALL OK?
10:28:58 < scurecode>  Scanner FOR SMTP-- Scanner For Root Scanner For Remote Desktop-RDP ITS
                       all Windows to USe i have AND Scanr Linux ROot and Win Root Scanner
                       Rapidshare Scanner C99 R57 Scanner Database Witch 1 Error you Connect
                       here Look All PeoPle Dont MSG for trade or For Share:) i want Just LR:)
                       to Sell ALL OK?
10:28:58 < maggii>  Script Php Mailer SMTP Orange.Fr Wanndo.Fr Optuss BigPond >>>>
10:28:59  * DUMPS` Selling dumps ( US , CA, FRance , SPAIN , Germany and some EU ) extracted
          from hotel database ( on Sale )! .. ( Verified +v user here ! you will not lose your
          money ... LOW LOW LOW PRICES ON BULK msg me now ) [illegible]
          [illegible]
10:29:00 < TradeCC>  wOOt3d is selling CC/CVV fullz dob/ssn/PIN US,UK, Lot of fresh unspammed
                     email, msg wOOt3d for more info
10:29:00 < maggii>  ShopAdmin USA Without cvv2 Uptime 3 Days 15 Orders day >>>>
10:29:02 < maggii>  Fullz/USA Citi Bank Bank OF America >>>>
10:29:02  * Skimmer For Sale Europe and united states DUMPS Platinum/gold/classic are available
          each for a price I accept only Webmoney/WesternUnion ! Nigerian rippers FUCK OFF! +@
          and admins can verify first !
10:29:02 < TradeCC>  MaStErBoY Is Selling AU Cvv2, Fulls , Paypal Accounts, SMTP, VNC ACCOUNTs
                     RDP ...
10:29:04  * GODy  Us\Uk\IT\Au\Ca => Cvv2 each 3$ - DUMPS SKIMMED AND GENERATED - SHOPADMINS -
          PAYPALS VERIFIED ! I GIVE PERVIEWS PROOFs SCREENSHOTS !
10:29:04 < maggii>  RapidShare Account 300 Days >>>>
```

Botnets

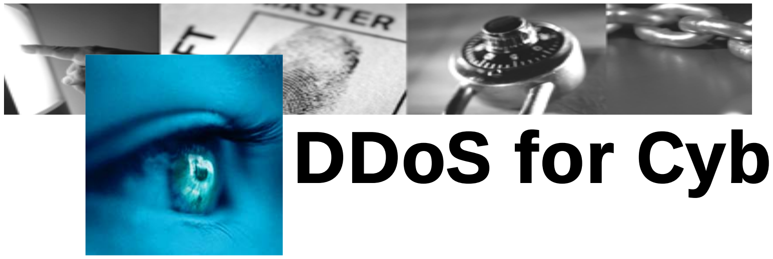
- **Software Robots**
  - Autonomous
  - Command and Control
  - IRC

- **Complex**
  - “Conficker” currently has estimated 9,000,000 hosts
    - Capable of 10 billion spam messages / day

Botnets

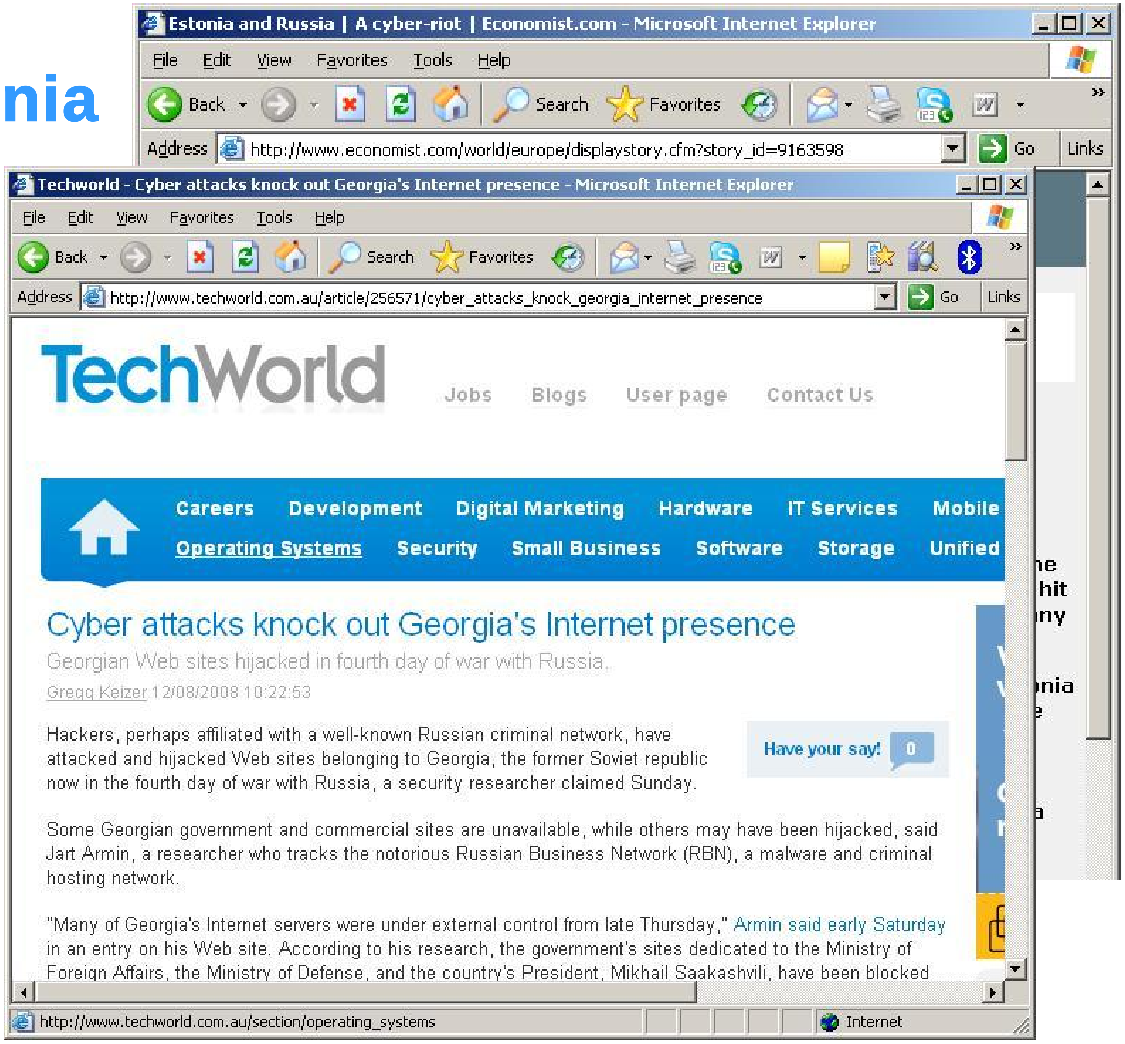


* *Source Wikipedia*



DDoS for Cyber Warfare

- RBN v Estonia
- RBN v Georgia



Estonia and Russia | A cyber-riot | Economist.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598
Go Links
Techworld - Cyber attacks knock out Georgia's Internet presence - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.techworld.com.au/article/256571/cyber_attacks_knock_georgia_internet_presence
Go Links
TechWorld
Jobs
Blogs
User page
Contact Us
Careers
Development
Digital Marketing
Hardware
IT Services
Mobile
Operating Systems
Security
Small Business
Software
Storage
Unified
Have your say! 0
http://www.techworld.com.au/section/operating_systems
Internet

Cyber attacks knock out Georgia's Internet presence

Georgian Web sites hijacked in fourth day of war with Russia.

Gregg Keizer 12/08/2008 10:22:53

Hackers, perhaps affiliated with a well-known Russian criminal network, have attacked and hijacked Web sites belonging to Georgia, the former Soviet republic now in the fourth day of war with Russia, a security researcher claimed Sunday.

Some Georgian government and commercial sites are unavailable, while others may have been hijacked, said Jart Armin, a researcher who tracks the notorious Russian Business Network (RBN), a malware and criminal hosting network.

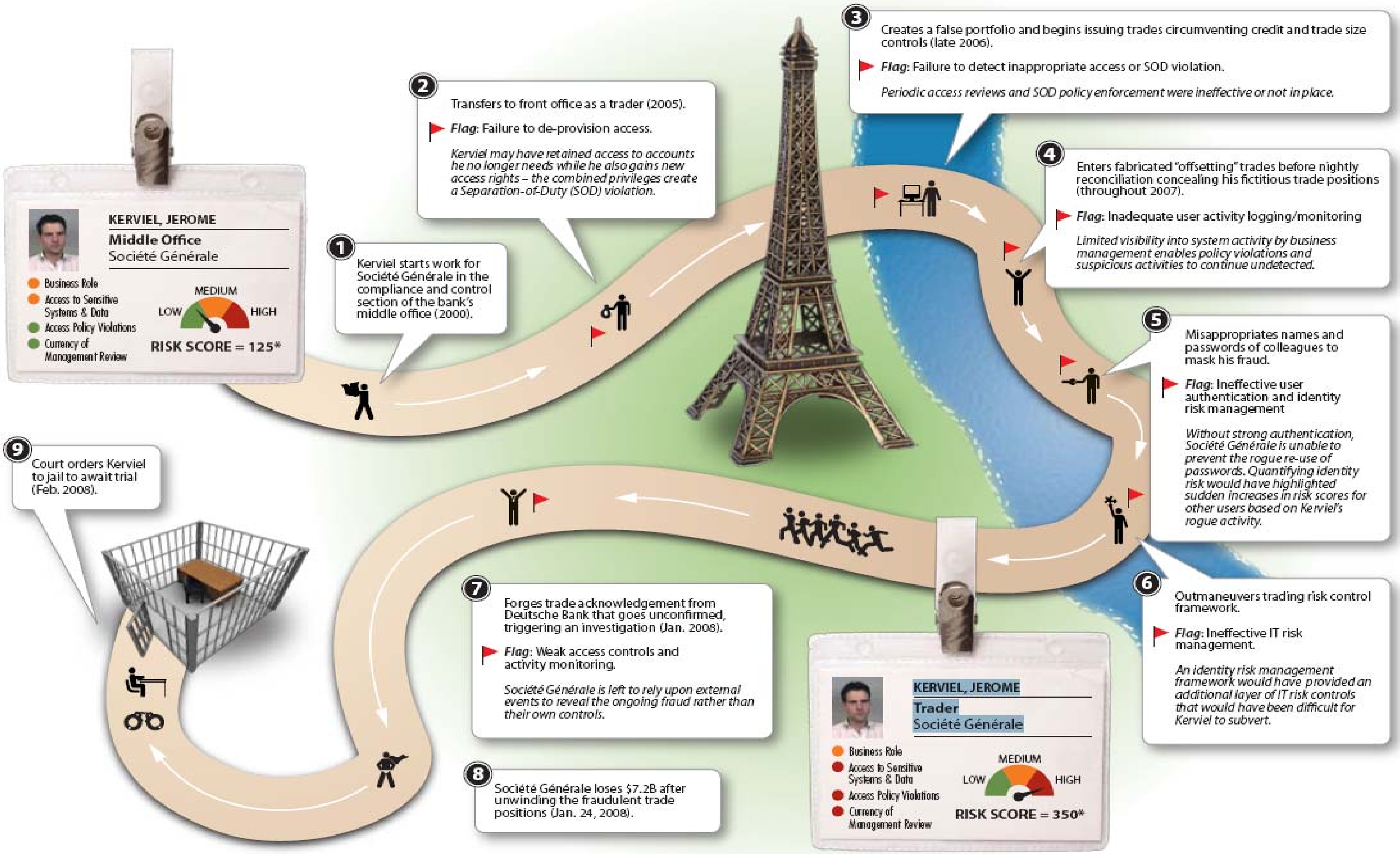
"Many of Georgia's Internet servers were under external control from late Thursday," Armin said early Saturday in an entry on his Web site. According to his research, the government's sites dedicated to the Ministry of Foreign Affairs, the Ministry of Defense, and the country's President, Mikhail Saakashvili, have been blocked

NET2S GROUP

Insider Threats

- **“Insiders”**
  - Generally trusted
  - Easy access to resources
  - Know how the system works
  - Understand data
- **Goals**
  - State / Military
  - Economic
    - Trade Policy / Secrets
  - Corporate
    - Acquire competitive advantage
    - Fraud

Rogue Trader - $7.2 Billion Loss



KERVIEL, JEROME
Middle Office
Société Générale

- ● Business Role
- ● Access to Sensitive Systems & Data
- ● Access Policy Violations
- ● Currency of Management Review

RISK SCORE = 125*

1 Kerviel starts work for Société Générale in the compliance and control section of the bank's middle office (2000).

2 Transfers to front office as a trader (2005).

Flag: Failure to de-provision access.

Kerviel may have retained access to accounts he no longer needs while he also gains new access rights – the combined privileges create a Separation-of-Duty (SOD) violation.

3 Creates a false portfolio and begins issuing trades circumventing credit and trade size controls (late 2006).

Flag: Failure to detect inappropriate access or SOD violation.

Periodic access reviews and SOD policy enforcement were ineffective or not in place.

4 Enters fabricated "offsetting" trades before nightly reconciliation concealing his fictitious trade positions (throughout 2007).

Flag: Inadequate user activity logging/monitoring

Limited visibility into system activity by business management enables policy violations and suspicious activities to continue undetected.

5 Misappropriates names and passwords of colleagues to mask his fraud.

Flag: Ineffective user authentication and identity risk management

Without strong authentication, Société Générale is unable to prevent the rogue re-use of passwords. Quantifying identity risk would have highlighted sudden increases in risk scores for other users based on Kerviel's rogue activity.

6 Outmaneuvers trading risk control framework.

Flag: Ineffective IT risk management.

An identity risk management framework would have provided an additional layer of IT risk controls that would have been difficult for Kerviel to subvert.

7 Forges trade acknowledgement from Deutsche Bank that goes unconfirmed, triggering an investigation (Jan. 2008).

Flag: Weak access controls and activity monitoring.

Société Générale is left to rely upon external events to reveal the ongoing fraud rather than their own controls.

8 Société Générale loses $7.2B after unwinding the fraudulent trade positions (Jan. 24, 2008).

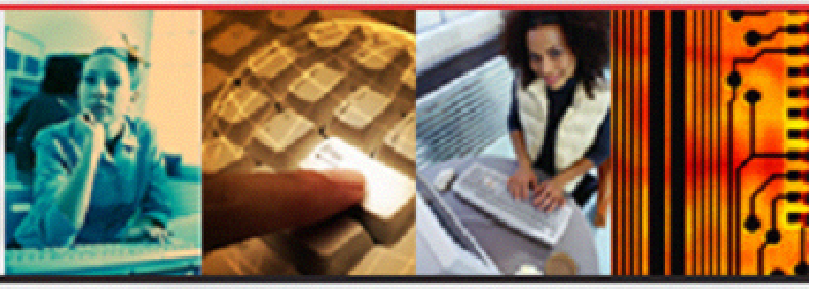
9 Court orders Kerviel to jail to await trial (Feb. 2008).

KERVIEL, JEROME
Trader
Société Générale

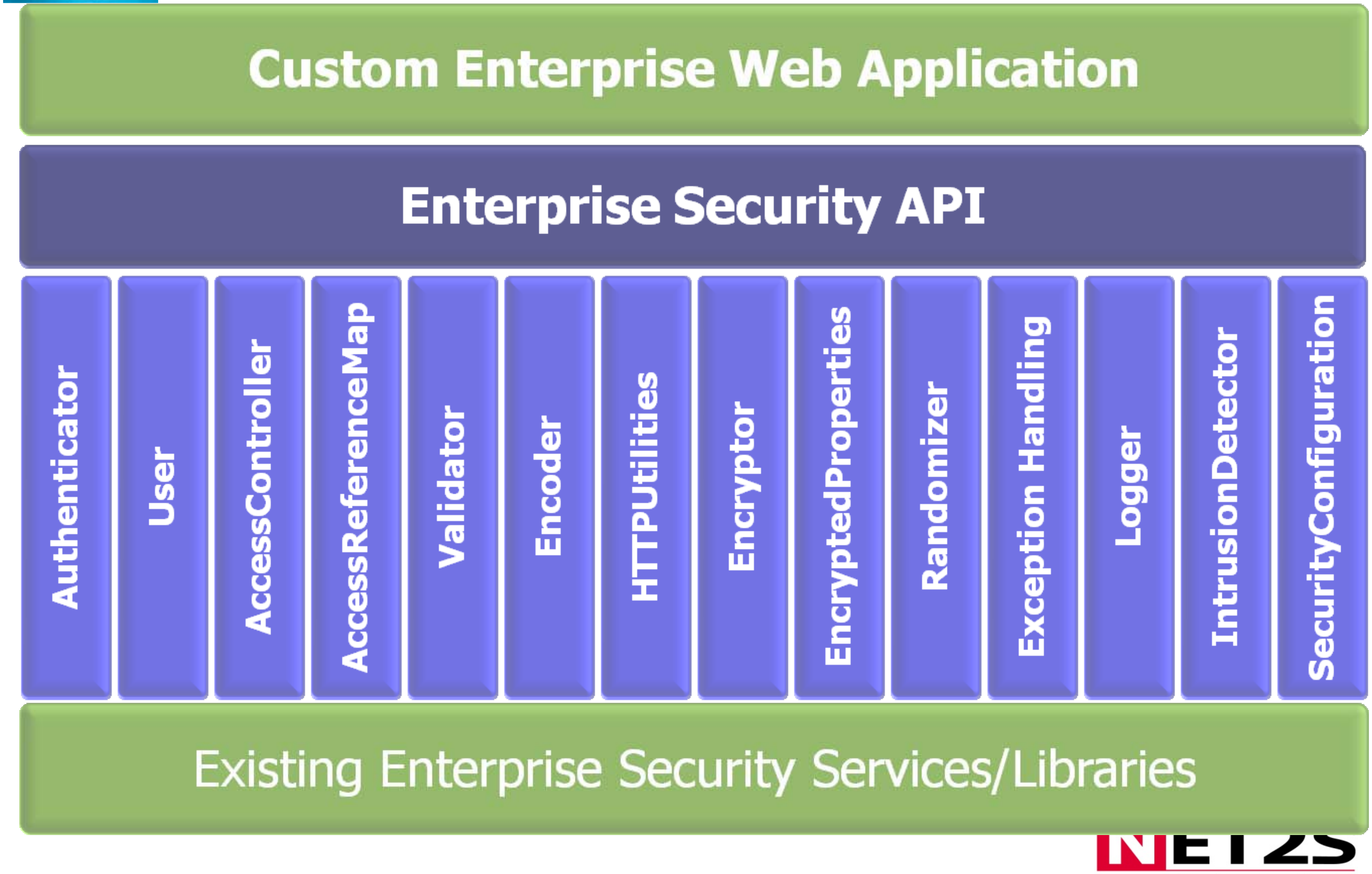
- ● Business Role
- ● Access to Sensitive Systems & Data
- ● Access Policy Violations
- ● Currency of Management Review

RISK SCORE = 350*

Demo



OWASP ESAPI



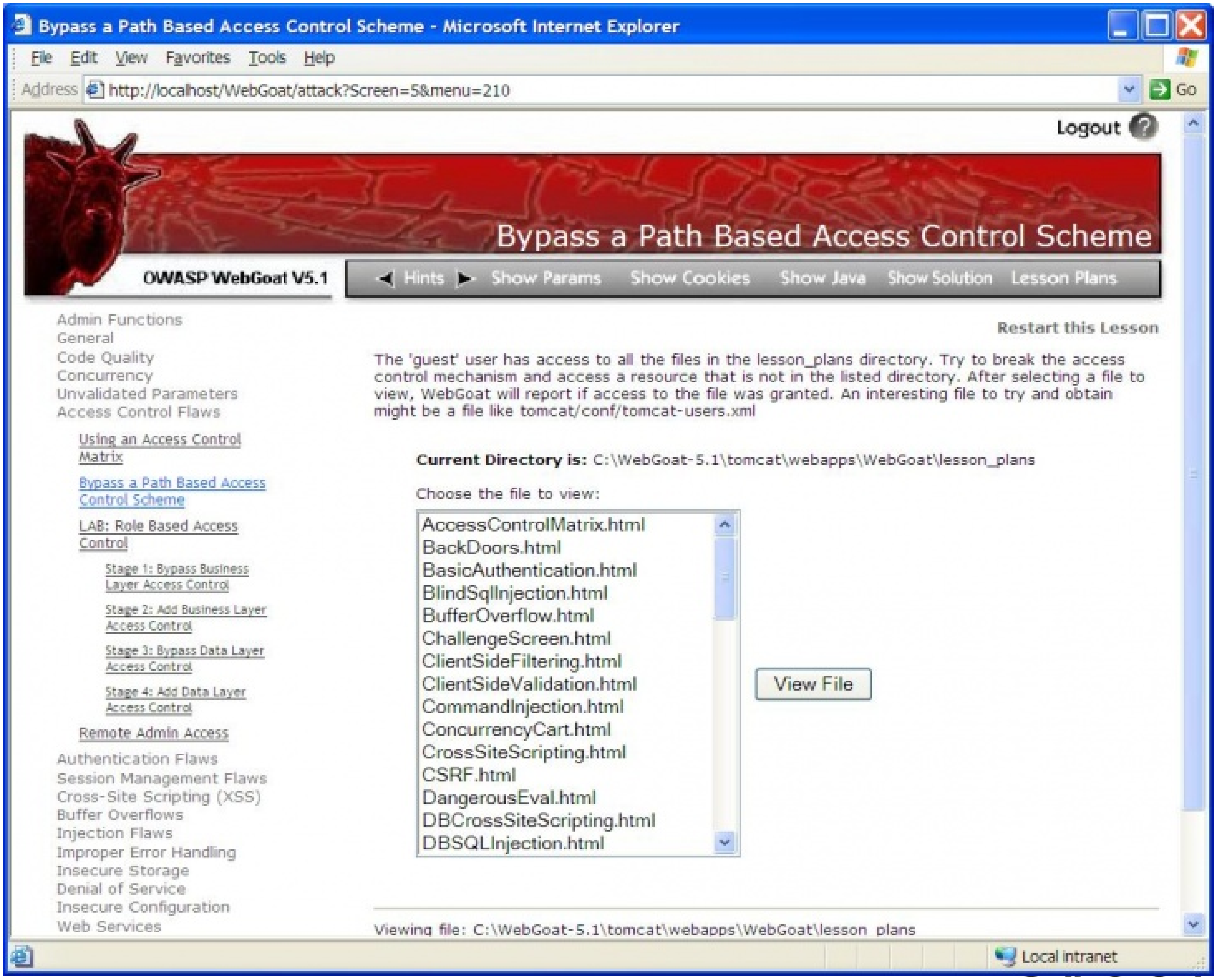
Custom Enterprise Web Application

Enterprise Security API

- Authenticator
- User
- AccessController
- AccessReferenceMap
- Validator
- Encoder
- HTTPUtilities
- Encryptor
- EncryptedProperties
- Randomizer
- Exception Handling
- Logger
- IntrusionDetector
- SecurityConfiguration

Existing Enterprise Security Services/Libraries

OWASP WebGoat



http://localhost/WebGoat/attack?Screen=5&menu=210

Bypass a Path Based Access Control Scheme

The 'guest' user has access to all the files in the lesson_plans directory. Try to break the access control mechanism and access a resource that is not in the listed directory. After selecting a file to view, WebGoat will report if access to the file was granted. An interesting file to try and obtain might be a file like tomcat/conf/tomcat-users.xml

Current Directory is: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Choose the file to view:

- AccessControlMatrix.html
- BackDoors.html
- BasicAuthentication.html
- BlindSqlInjection.html
- BufferOverflow.html
- ChallengeScreen.html
- ClientSideFiltering.html
- ClientSideValidation.html
- CommandInjection.html
- ConcurrencyCart.html
- CrossSiteScripting.html
- CSRF.html
- DangerousEval.html
- DBCrossSiteScripting.html
- DBSQLInjection.html

Viewing file: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Learning

- **Hacking Challenges**
  - http://www.hackthissite.org
  - http://www.dareyourmind.net

- **Education / Tools**
  - http://www.owasp.org

Q+A