18th Annual FIRST Conference
June 25–30, 2006
Baltimore, Maryland USA

What You Don't Know That You Don't Know

Arjen de Landgraaf
Co-Logic Security Ltd (New Zealand)

Rules of Engagement

We are <u>not</u> allowed to:

- Pour hot oil and feathers
- Shoot Arrows
- Throw Stones
- Chuck dead cows
- Even slightly harm them

We Can Only Defend the Gates

- Routers
- Firewalls
- Anti Virus
- Anti DoS
- Anti Anything

How To Stop Them

- Check and lock the Gates
- Detect them when they are inside.

Logs

IDS

IPS

Alarms

And when they are inside

- Yes, **then** we can fight them
- As long as we know they are here
- And where they exactly are
- And we still cannot fight them according to their rules.

With any Breach or Compromise, Damage is Inevitable

Today's Marketplace

Demand is Market and Marketing Driven

We ALL Need to Compete in a Global Economy

Visitors are encouraged to visit, enter, browse, read, request, search, look, try to buy, trade, test. AND BUY

Today Marketing drives New Development

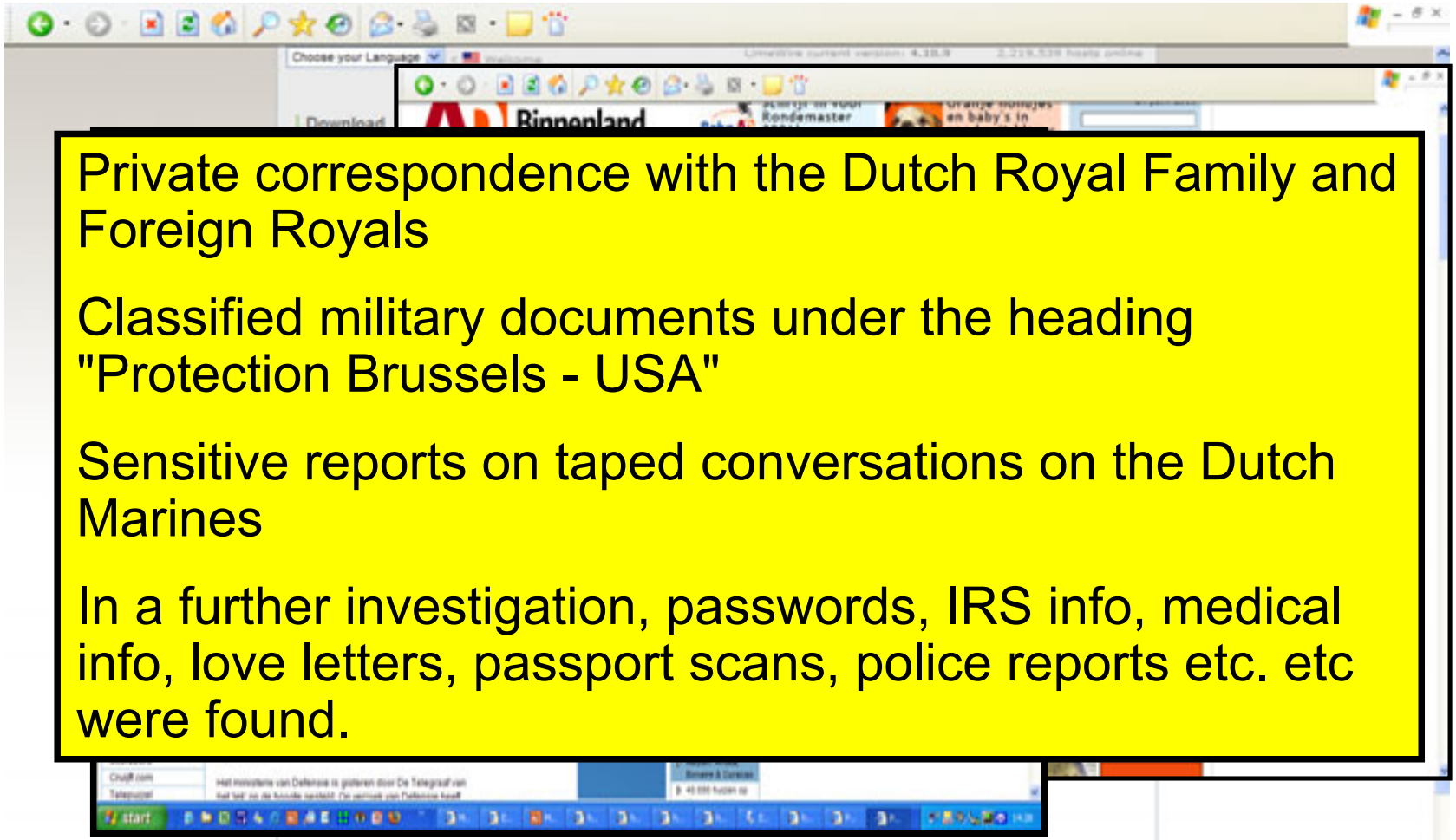
- Grow, hold and increase market share, optimized returns, increased competition on a global scale
- To survive and thrive, openness, ease of access, simplicity is key

Marketing and Sales is now Driving Web (and Systems) Development

Today's Programmers need to be Visual Artists

- Web design, delivery and functionality as USP
- Ease of use for untrained visitors
- Driven by Market

Example 1 – AIVD Gate



Private correspondence with the Dutch Royal Family and Foreign Royals

Classified military documents under the heading "Protection Brussels - USA"

Sensitive reports on taped conversations on the Dutch Marines

In a further investigation, passwords, IRS info, medical info, love letters, passport scans, police reports etc. etc were found.

Example 2 – Web Applications

Example 3 – The Rocky Phisher

Some of the Sites Targeted over last 6 months

Alliance and Leicester
Barclays
Citibank
Commerzbank (Germany)
Deutsche Bank
EBay
Halifax
HSBC
Dresdner Bank
Westpac Corporation (NZ / Aus)
ANZ (Australia / NZ Bank)
Suncorp Internet Banking
Hypovereigns Bank (Germany)
NAB - National Australia Bank
SEEK.COM.AU (Non Bank - Australian Job seekers site)
O2 (non banking UK)
UNSEEN (non banking UK)
Commonwealth Bank
APO Bank (German)
BNZ - Bank of New Zealand
NCUA (Australia)
MBNA Europe
Nationwide Building Society (UK)
Macquarie Bank (Australia)

No-One has Been Able to Stop Him Yet

Not one IT-Security Company, CERT, legal body or government department in the World has yet been able to stop the

“Rocky” phishing attacks

Rocky

- /r1/
- Phishing Email format
- Quality – professional
- Use of Language (s) – Excellent
- Each week new target
- .us .biz .info
- USA, China, Thailand, Republic of Korea, Turkey
- http://www.macquarie.com.au.au.retail.customercare.lesbaz.info/r1/conf.asp/
- http://www.macquarie.com.au.au.retail.customercare.romnid.info/r1/conf.asp/

Rocky

- Earlier samples keylogging trojan
- Now just VNC / radmin
- Apparently servers only pass the Request on. Either simple Port forwarding or as Reverse Proxy.
- This conclusion is based on the fact that under several servers with completely different IPs (thus different Netblock) exactly the same data files are located.
- In addition submit.php and verify.php on one now .asp
- nix servers lie (to recognize by the path in the error message). Further have all SSL host on the IPs exactly the same certificate fingerprint.

Rocky

- genezi.biz goverkk.biz kiosi.biz koiller.biz partnerz.biz - portfill.biz sioko.biz tekasi.biz lali22.info **kilo88.us** **catndog.us** artaf.biz simi00.biz kileof.biz maddr.info cudey.biz romnid.info lesbaz.info

- /r1/asp/
  /r1/b/
  /r1/c/
  /r1/cj/
  /r1/h/
  /r1/n/
  /r1/p/
  /r1/v/
  /r1/vr/

  Very structured worker – B / C etc.

Rocky

- 211.199.252.187:180/
  211.32.14.248
  81.215.229.191
  211.55.216.176
  218.159.245.121
  210.183.80.177
- Apache/1.3.34(Unix) mod_ss/2.8.25 OpenSSL/0.9.7a PHP/4.42 mod_perl/1.29 FrontPage/5.0.2.2510

- .php or .asp

Rocky

- Interesting ports on 218.159.245.121:
  (The 1662 ports scanned but not shown below are in state: closed)
  PORT STATE SERVICE
  25/tcp open smtp
  80/tcp open http
  110/tcp open pop3
  135/tcp filtered msrpc
  139/tcp filtered netbios-ssn
  180/tcp open ris
  445/tcp filtered microsoft-ds
  1025/tcp open NFS-or-IIS
  4444/tcp filtered krb524
  4899/tcp open radmin
  5000/tcp open UPnP
  6004/tcp open X11:4

- VNC and Radmin

Rocky

- Radmin- password times-out after a couple of attempts in a one-minute delay so brute forcing is not an option.

  Zombie servers with complete control over them
- (if he can install a web server he will have iig root/administrator access).

- Sites often use JavaScript tricks to replace the browser toolbar and disable keyboard functions such as Cut and Paste.

Macquarie Bank

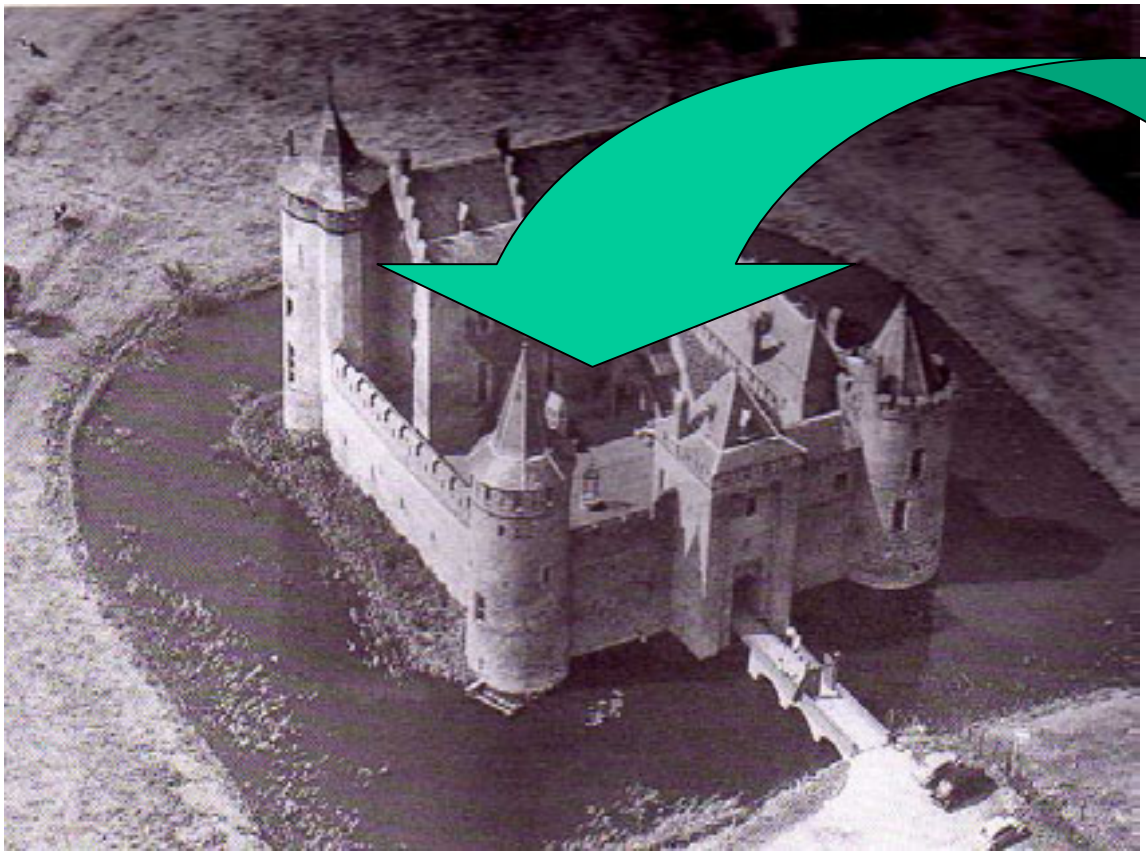
- 218.69.98.89
- inetnum: 218.67.128.0 - 218.69.255.255
  netname: CNCGROUP-TJ
  country: CN
  descr: CNCGROUP Tianjin province network

Traditional Armour and Defence Style is Not Enough

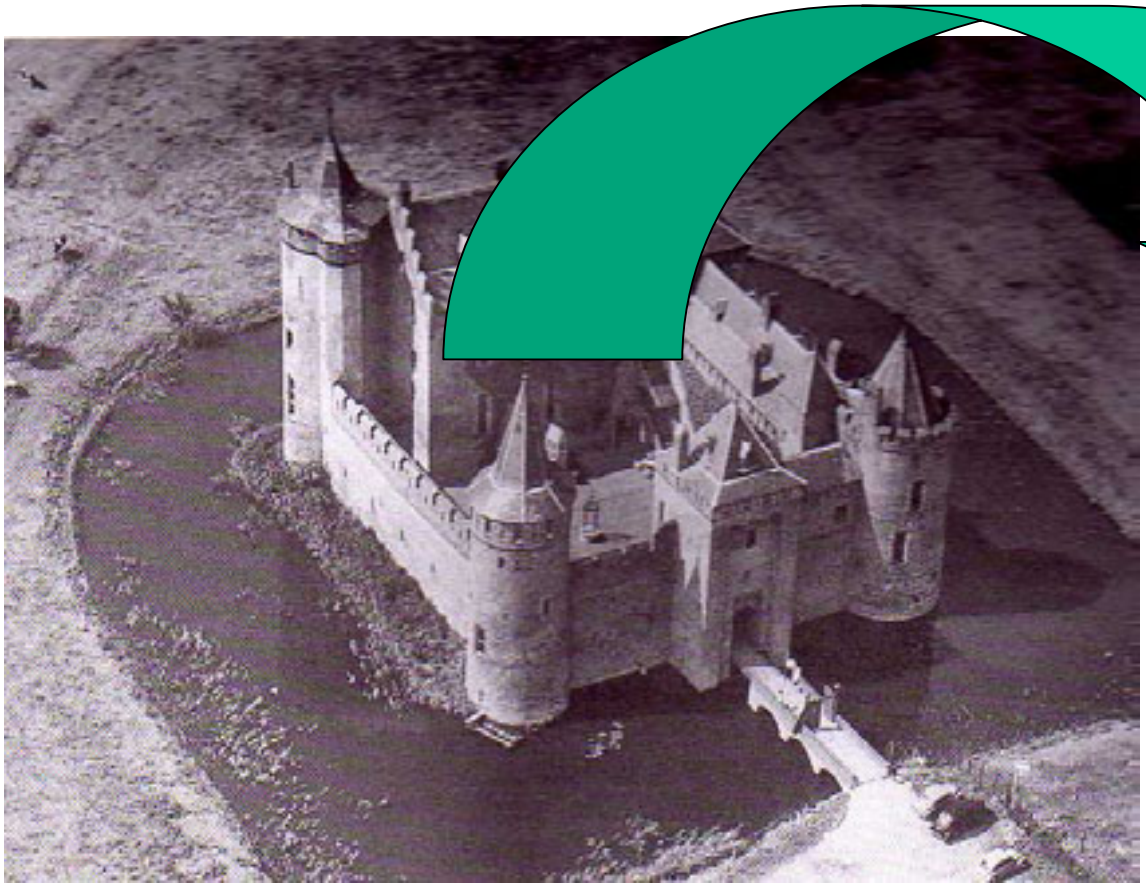
Changed landscape

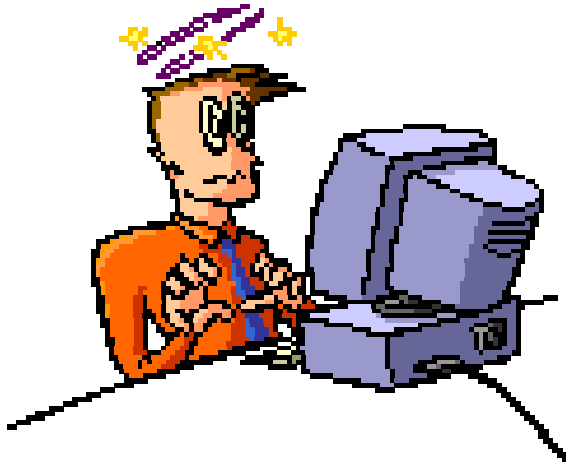
- Less viruses, more phishes
- More Web App attacks
- More Direct Attacks
- Assets as Reward

So you got to let them in



And you got to let them out





And….. You Also Need To Stop These

How to Get to Know – What You Don't Know You Don't Know?

In the past – Finance Department

What is exactly running in your patch?

What Scripts and objects are running wild?

New Age Web Designers and programmers:

Rounding up black cats in a dark room

Get them to REALLY understand

Unaware (business, not IT) Teleworkers

What Can you Do?

Create A Clearing around your Castle to see what's coming

- **Know your Weaknesses**
- **Where are your potential vulnerabilities**
- Where can they attack you?
- **See them Coming**

Building Effective Relationships between CSIRTs and Law Enforcement
18th Annual FIRST Conference
Thursday – June 29th, 09:10

Brian Nagel, assistant director of the US Secret Service Office of Investigations will present a keynote address,

"Building Effective Relationships between CSIRTs and Law Enforcement,"

In an endeavour to bridge what are seen as cultural and operational differences between LE and CSIRT approaches to security.

Questions?

www.e-secure-it.com