



## Cyber Threats – Setting the Scene



**ASSOCIATION OF IRISH RISK MANAGEMENT**  
A FORUM FOR THE INTERCHANGE OF IDEAS



# Paul C Dwyer – BIO

**paul C dwyer**  
SECURITY GRC & CYBER CRIME ADVISOR

Paul C Dwyer is an internationally recognised information security expert with over 21 years experience.

A certified industry professional by the International Information Systems Security Certification Consortium (ISC2) and the Information System Audit & Control Association (ISACA) and recently selected for the IT Governance Expert Panel.

Paul's credentials include:

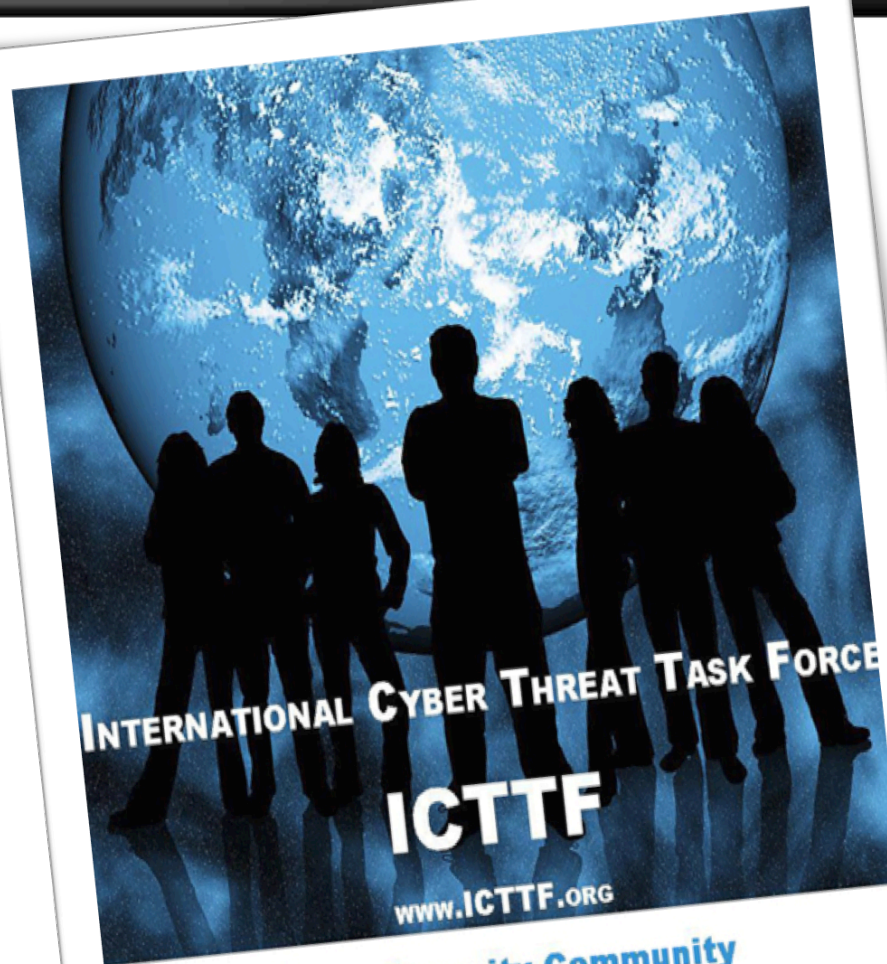
- -Qualified Hacker
- -SOX (SAS70) Auditor
- -ISO 27001 Lead Auditor
- -BS25999 / BCP Expert
- -Forensic Investigator
- -PCI DSS Specialist
- -Prince2

He has worked and trained with such organisations as the US Secret Service, Scotland Yard, FBI, National Counter Terrorism Security Office (MI5), is approved by the National Crime Faculty and is a member of the High Tech Crime Network (HTCN).



# ICTTF.org

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



## Cyber Security Community



Photo Albums



Blogs



Events



Groups



Forums



Video Sharing



Chat & IM



Classifieds



Polls



Mobile



# Cyber Threats - Blurred Lines

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR





# What is Cyber Crime?

Cyber crime or computer crime as it is generally known is a form of crime where the Internet or computers are used as a medium or method to commit crime which includes **hacking, copyright infringement, scams, denial of service attacks, web defacement and fraud.**



In our heavily networked world, **cyber attacks represent a 24/7/365 threat.**

# What is Cyber Warfare?

*“actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”*

- “Digital Infrastructure....Strategic National Asset”  
President Barack Obama
- May 2010 – Pentagon – Cybercom
- UK - a cyber-security "operations centre" (GCHQ)
- “Fifth Domain” The Economist



# What is Cyber Scum?

- Paedophiles
- Stalkers
- Groomers

Recent analysis in Ireland:

“Over 1,000 people in 30 days, of that number 697 were spotted 1 to 2 times. 337 were spotted 3 or more times” Primetime RTE





# Categories of Attacks

- **Criminal Attacks** (fraud, theft and grand larceny, identity theft, hacking, extortion, phishing, IPR and copyright theft, piracy, brand theft, 'spoofing')
- **Destructive Attacks** (cyber-terrorism, hackers, ex-employees, vengeful individuals, cyber war, cyber-vandals, anarchists, viruses)
- **Nerd Attacks** (Denial of Service attacks, publicity hounds, adware)
- **Espionage Attacks** (data and IPR theft, spyware)



Each sector has its own niches criminals

- **Phishers** - consumer financial services
- **Industrial spies** — IP companies
- **(H)Activists** — social impact they disapprove
- **Hackers** — scalp for prestige
- **Cyber terrorists** — hurt the west
- **Fraudsters** — any to siphon cash



# Hacktivism?

paul C dwyer  
SECURITY GRC & CYBER CRIME ADVISOR

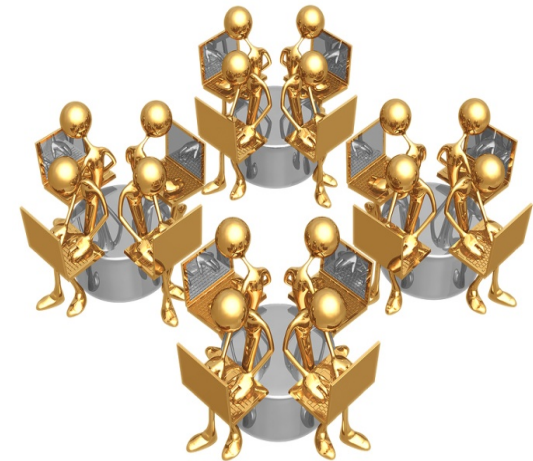




# Threat Groups

Threats originate with people.

- **Criminals** (thieves, fraudsters, organised crime)
- **Malefactors** (hackers, vandals, terrorists, cyber-warriors)
- **Spies** (commercial and governmental)
- **Undesirables** (scam artists, spammers, 'ethical' hackers)
- **The incompetent, or the simply unaware**  
(staff, contractors, customers and other third parties)



These people are found both inside and outside an organisation and can exert an influence out of proportion to their numbers

# Computer Misuse Legislation

- Computer misuse legislation is relevant in two ways:
- authorities and organisations can take action under it against cyber-criminals
  - organisations have to ensure they comply with it themselves.
  - Directors can be personally accountable for any compliance failures.



# Convention on Cyber Crime

Council of Europe adopted a Convention on Cyber crime that identified and defined internet crimes:

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices);
- computer-related offences (computer-related forgery, computer-related fraud)
- content-related offences
- offences related to infringements of copyright and related rights





- All organisations need to be aware of the Convention's provisions in article 12, paragraph 2: *'ensure that a legal person can be held liable where the lack of supervision or control by a natural person...has made possible the commission of a criminal offence established in accordance with this Convention'*.
- In other words, directors can be responsible for offences committed by their organisation simply because they failed to adequately exercise their duty of care.

# Is it Real?





# Reasons for Escalation

It's a business with an excellent **economic model**.











Other reasons, you name it:

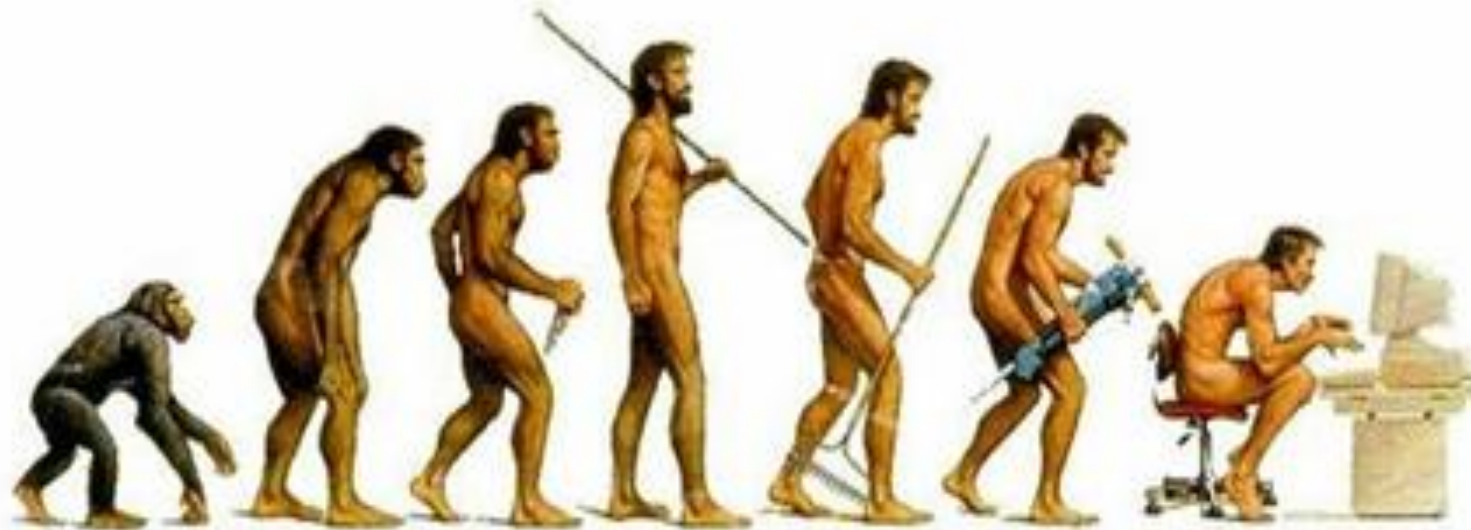
- Technology
- Internet
- Recession
- “A safe crime”
- It's easy to get involved
- Part of Something



# Distribute, Wholesale, Resell

The most common 'positions' or specializations according to the FBI are:

-  **1. Programmers.** Who develop the exploits and malware used to commit cyber-crimes.
-  **2. Distributors.** Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
-  **3. Tech experts.** Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.
-  **4. Hackers.** Who search for and exploit applications, systems and network vulnerabilities.
-  **5. Fraudsters.** Who create and deploy various social engineering schemes, such as phishing and spam.
-  **6. Hosted systems providers.** Who offer safe hosting of illicit content servers and sites.
-  **7. Cashiers.** Who control drop accounts and provide names and accounts to other criminals for a fee.
-  **8. Money mules.** Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
-  **9. Tellers.** Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
-  **10. Organization Leaders.** Often "people persons" without technical skills. The leaders assemble the team and choose the targets.



# Malicious Tool Evolution



# Crimeware Toolkits

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR





# Crimeware in the Cloud



Just-B

## PII



## PII

5 Credits  $\approx$  1 US Dollar

Date of Birth: **50.0 Credits**

Credit Card Balance: **1.5 Credits**

Mother's Maiden Name: **50.0 Credits**

Social Security Number: **20.0 Credits**

Driver's License Number: **50.0 Credits**

# Example of Crimeware

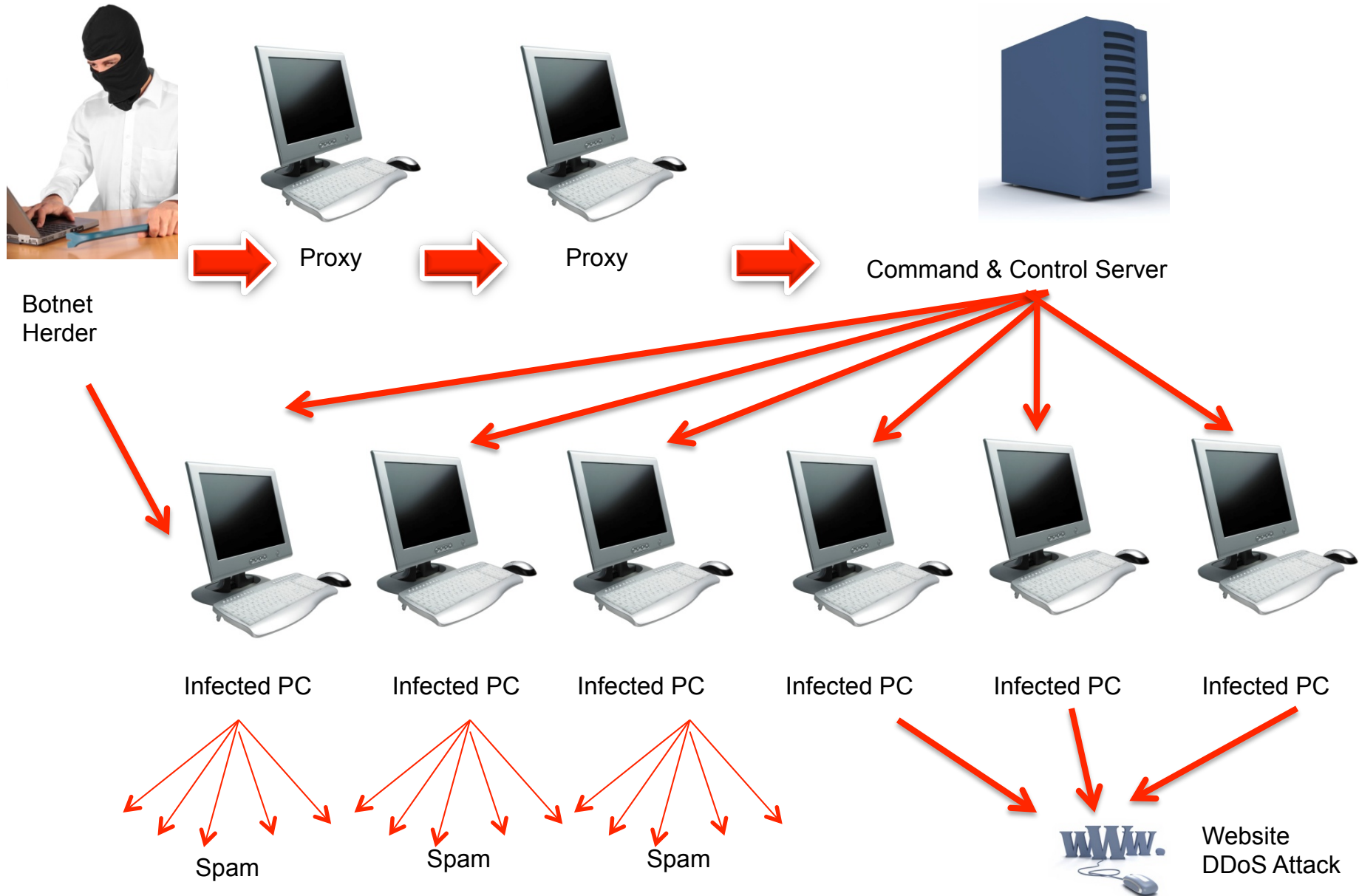


Tools, Tutorials, Services (Rent & Buy)

Spyeye \$500



# Botnets (Rent or Own)



# Spyeye – Toolkit

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



Botnet  
Herder



Proxy



Spyeye C & C Server



# Install Command and Control

Скриншот веб-интерфейса администратора в Mozilla Firefox. Адресная строка: adminko2.

Верхняя панель инструментов содержит следующие кнопки:

- 2009 12/30 05:33:17
- Create task for Billing
- Modify Cards
- Tasks Statistic
- Bots Monitoring
- Settings
- Ban Bots
- Create task for Loader
- Create task for Knocker

Центральная часть интерфейса:

- Круглая иконка с различными символами (звезда, ракетка, дискета, монитор) и кнопка **Show All**.
- Круглая иконка с ракеткой и кнопка **eSellerate**.

Заголовок таблицы: Global tasks for billing eSellerate

ID	Note	Start Time	Finish Time	Bots Count	Tasks Processing (%)	[Detail info]	[Controls]
305	test	2009-12-30 05:31:05	2009-12-30 05:33:05	1	<div><div></div></div>		

Заголовок таблицы: Bots with cards for Global task # 305

[Restart]	[New time]	ID Task	Planned Time	Begin Time	End Time	E-Mail	Message Log	Client's info	Id Bot
		4084	2009-12-30 05:30:54	2009-12-30 05:32:17		adminko2@yandex.ru	ERROR	5.1.2600 8.1.101.18702 Admin	

Статус: Готово

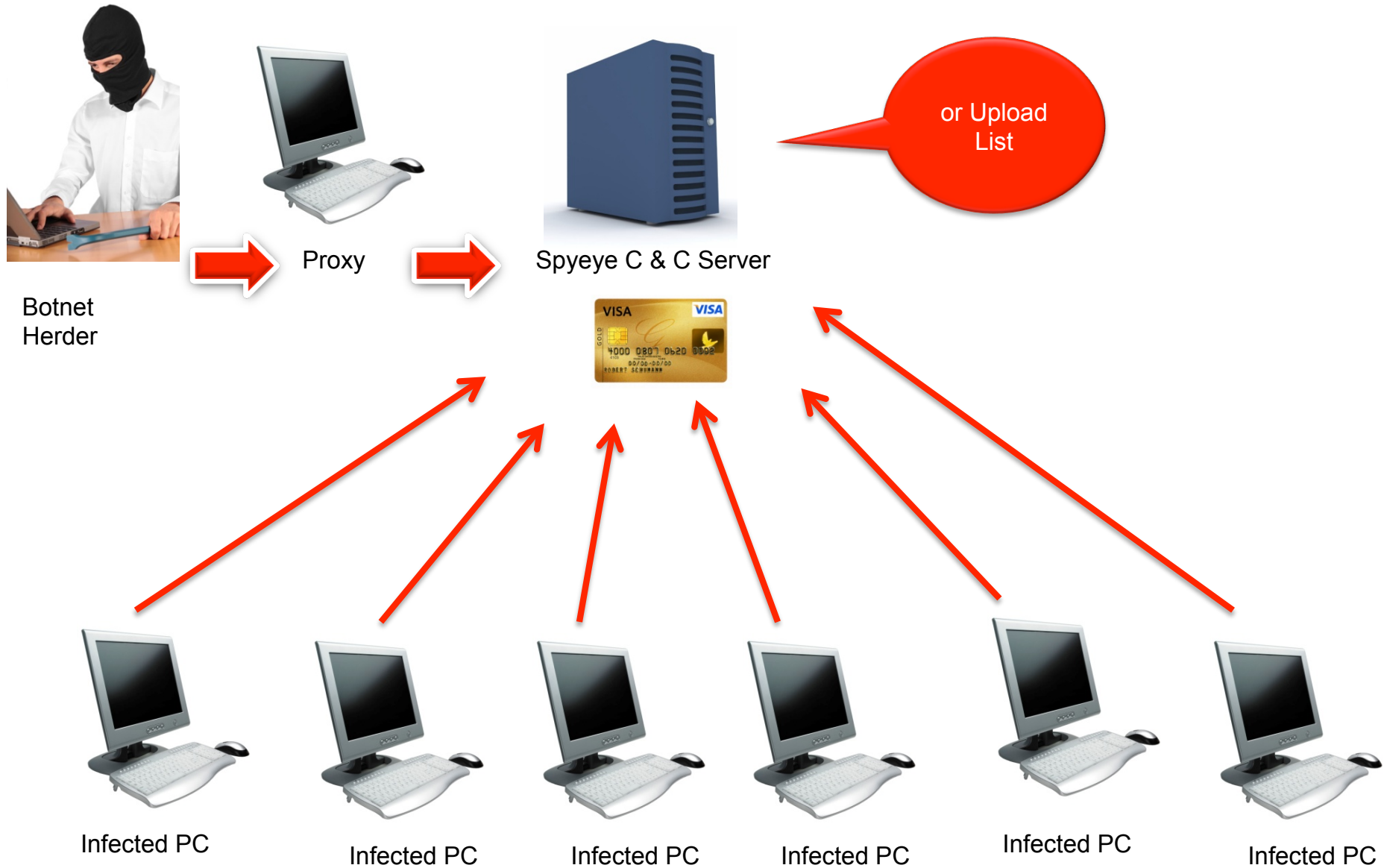
Панель задач (Taskbar):

- Пуск
- DebugView on V...
- СН 1 - Mozilla Fir...
- u/screencamera
- 2 5лсКНОТ
- EN
- 1:33

Дополнительная информация: Fiddler: Disabled

# Get CC Info

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



# Place Something For Sale

paul C dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



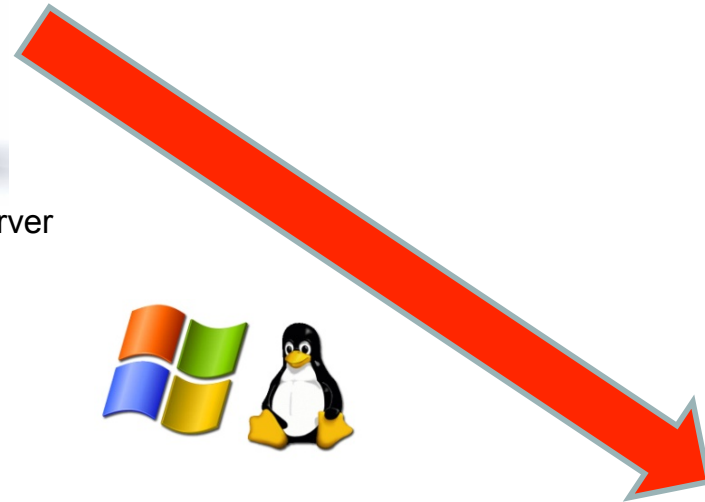
Botnet  
Herder



Proxy



Spyeye C & C Server



Uploads, Renames and  
Claims Ownership of  
Software Utility For Sale on  
a popular download store



# Automate Transactions

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



Botnet  
Herder



Proxy



Spyeye C & C Server



Spyeye automates  
purchases by form filling at  
intervals to avoid detection  
sing the stolen credit card  
information



# Clean Money

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



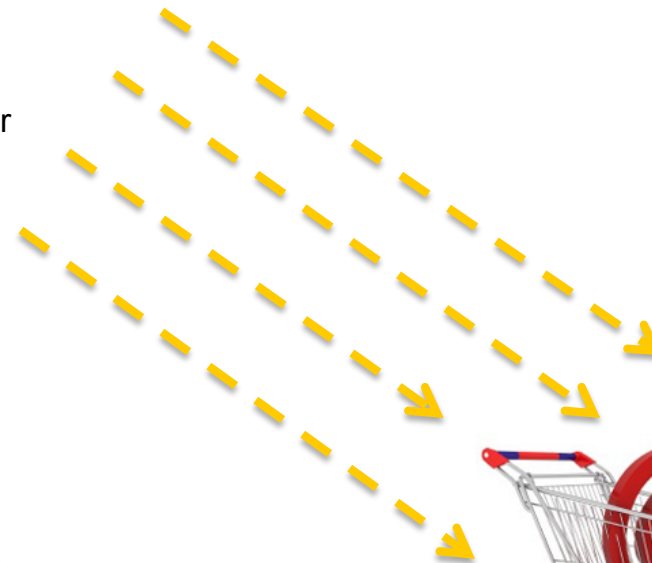
Botnet  
Herder



Proxy



Spyeye C & C Server







# Billing Hammer Module



## Spy Eye v1.2




2010  
09/15  
21:55:58




Find INFO




Statistic




FTP accounts



Settings



Screen shots




BOA Grabber



VISA CC Grabber



Certificate Grabber



27285 k  
+551300

### Get Credit Cards

+231

Bot GUID :


Report date region :  
14/09/2010 ... 15/09/2010

Data :

Limit :

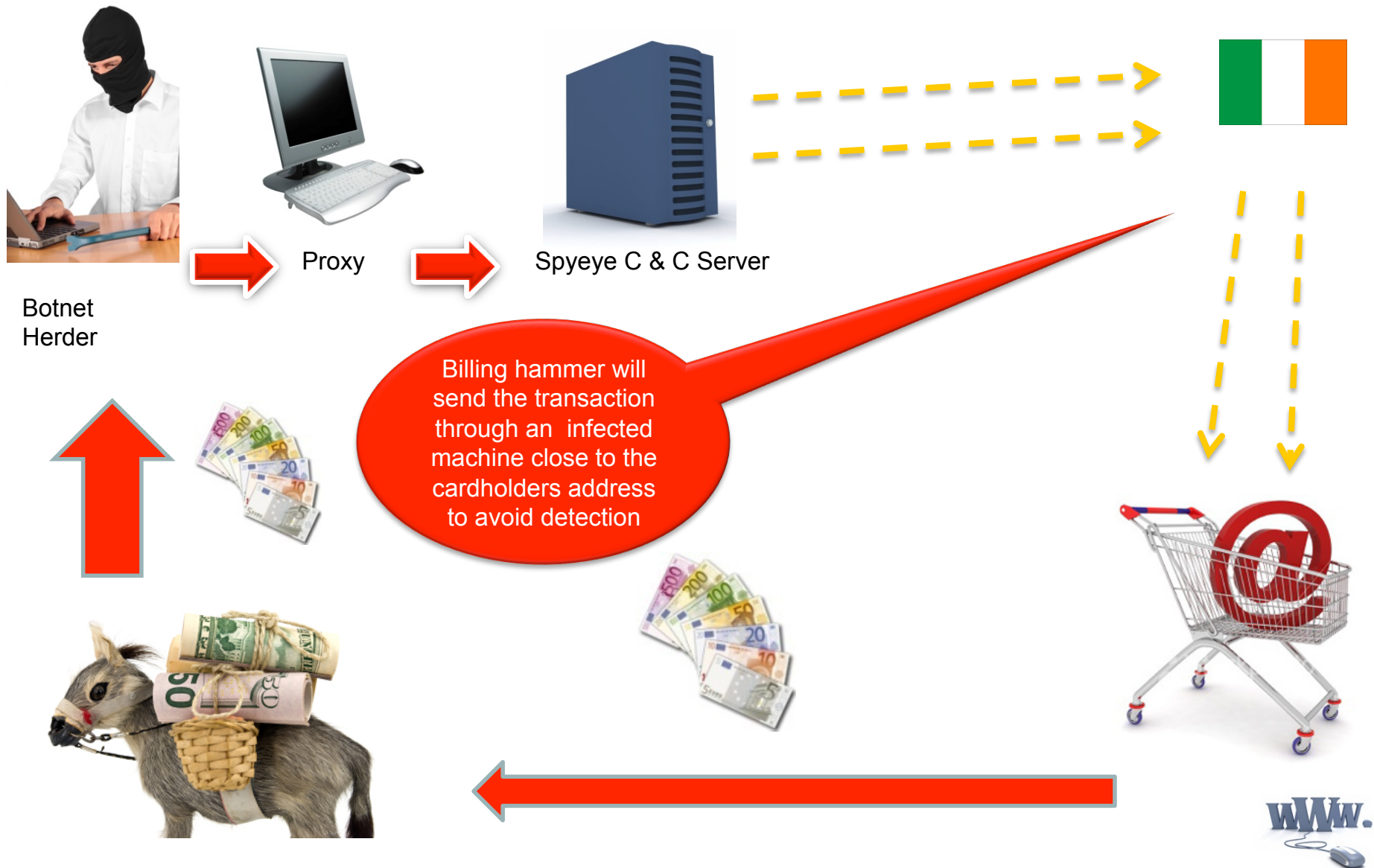
with CVV only :  
☒

with Address only :  
☒

id	bot_guid	url	date_rep
	sid!SID-PC!36469FDA	https://www.namecheap.com	2010-09-14 22:43:32

```
cc_type=VISA
cc_number=4862381234567890
ccexp_month=04
ccexp_year=11
cc_cvc=818
billing_name=John Doe
req_id=67371.57
regid=113574-d071e1d3e4
chargetotal=10.16
payment_method=CC
billing_first_name=John
billing_last_name=Doe
billing_organization=none
billing_address1=1234 Main St
billing_address2=
billing_city=Navarre
billing_state=FL
billing_zip=32566
billing_country=US
billing_email=johndoe@fudmail.com
billing_phone=+1 9045551234
Submit=Charge and Process >>
```

# Avoid Detection



# Closer to Home

- Cybercrime costs £27 billion a year in the UK
- £1,000 a second
- 170,000 ID's are stolen each year – 1 every th
- Theft of IP £9.2 billion (pharmaceuticals, biotechnology, electronics, IT and chemicals)



- Industrial Espionage £7.6 billion
- Citizens £3.1 billion
- Government £2.2 billion



# UK Response

*“the answer lies in private firms and the Government working together to disrupt criminal networks rather than prosecution”*

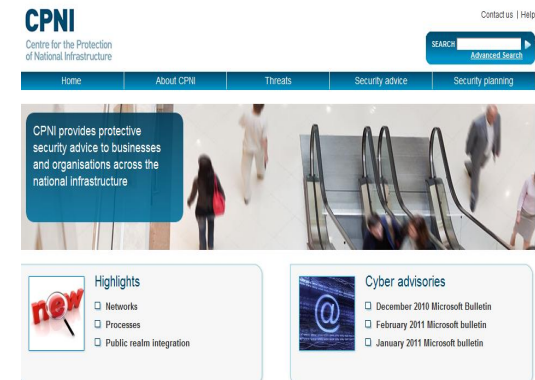
- Cyber attacks on the UK's information technology systems were identified in last year's Strategic Defence and Security Review (SDSR) as **one of the four most serious threats to national security**, alongside terrorism, natural disasters and major accidents.
- Backed by **£650 million in new Government funding** announced in the SDSR, the National Cyber Security Programme will develop means of responding to threats from states, criminals and terrorists.



Security Minister  
Baroness Neville-Jones



- Prime Minister David **Cameron** recently met representatives of some of Britain's **biggest private companies** to work with the Government on protecting the country against cyber attack.
- Foreign Secretary William Hague and Baroness Neville-Jones also took part in the talks at 10 Downing Street with firms including **British Airways, Centrica, the National Grid, BT, Barclays, HSBC and GSK.**
- They agreed to form a working party to look at detailed proposals for action, drawing on expertise from the private sector.



# NATO

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



# “The Daddy” - History

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR



Dark Market



**Keith Mularski:**  
FBI Senior Cyber Crime Agent  
AKA Master Splyntr



# Original Crew

paul C dwyer  
SECURITY GRC & CYBER CRIME ADVISOR

Turkish LE: 2008



Cagatay Evyapan – Cha0



Type of Service or Product	Description	Average Price (USD)
US Dumps Track1	USA, Name, Account Number, Expiration Date, CW	8
US Dumps Gold Track1	USA, Name, Account Number, Expiration Date, CW	20
US Dumps Discover Track1	USA, Name, Account Number, Expiration Date, CW	8
EU Dumps Track1	European, Name, Account Number, Expiration Date, CW	50
EU Dumps Gold Track1	European, Name, Account Number, Expiration Date, CW	90
AP Dumps Track1	Asian/Pacific, Name, Account Number, Expiration Date, CW	40
AP Dumps Gold Track1	Asian/Pacific, Name, Account Number, Expiration Date, CW	50
CD Dumps Track1	Canadian, Name, Account Number, Expiration Date, CW	10
CD Dumps Gold Track1	Canadian, Name, Account Number, Expiration Date, CW	25
Plastics Embossed	Counterfeit Credit Cards with Embossing on card	50
Plastic Banks	Counterfeit Credit Cards	40
Plastics w/ Halo	Counterfeit Credit Cards with security holograms	75
COBs	Change of Billing Information	60
Hologs	Holograms	5
Full Infos	Track 1 info plus email address, DOB, MMN	15
Enrolls	Information to apply for new accounts	45
Skimmed	Duplicated magnetic track data from POS (Restaurant, Hotel, Retail, etc.)	40
Credit w/ PIN	Credit Card information plus PIN	175
Track2 w/ CVV2	Track 2 data plus the security code imprinted on the signature panel card	2
Visa / MC CC# w/CVV2	Transaction information plus security code	3
Balance Checking	Service provided by vendor to check available balance on stolen accounts	2
Phishing Pages	Scam pages of legitimate websites	100
Bank Logins	Compromised bank login username and passwords to bank cardholders	100



# Pump & Dump

- SPAM Campaign
- Increasing in scale and sophistication
- Occurs in under one week
- Brokerage account(s) (stolen)
- Email sent (graphic) with nonsensical text “Bayesian poisoning”
- People buy, stock rises, scammer sells
- Example \$.88, \$1.28, \$.13



# What is mainstream now?

- Social Network / Media Crime
- DDoS
- Child Exploitation Material
- PABX Fraud
- RansomWare
- Trojans/Malware
- Identity Theft



# Cyber Threats are Social

paul C dwyer  
SECURITY GRC & CYBER CRIME ADVISOR





# Facebook Statistics



## People on Facebook

More than 500 million active users  
50% of our active users log on to Facebook in any given day  
Average user has 130 friends  
People spend over 700 billion minutes per month on Facebook

500 Million Users

## Activity on Facebook

There are over 900 million objects that people interact with (pages, groups, events and community pages)  
Average user is connected to 80 community pages, groups and events  
Average user creates 90 pieces of content each month  
More than 30 billion pieces of content (web links, news stories, blog posts, not photo albums, etc.) shared each month.

900 Million Objects

## Global Reach

More than 70 translations available on the site  
About 70% of Facebook users are outside the United States  
Over 300,000 users helped translate the site through the translations application

70 Languages

## Platform

Entrepreneurs and developers from more than 190 countries build with Facebook Platform  
People on Facebook install 20 million applications every day  
Every month, more than 250 million people engage with Facebook on external websites  
Since social plugins launched in April 2010, an average of 10,000 new websites integrate with Facebook every day  
More than 2.5 million websites have integrated with Facebook, including over 80 of comScore's U.S. Top 100 websites and over half of comScore's Global Top 100 websites

Installation of 20 Million Applications a Day

## Mobile

There are more than 200 million active users currently accessing Facebook through their mobile devices.  
People that use Facebook on their mobile devices are twice as active on Facebook than non-mobile users.  
There are more than 200 mobile operators in 60 countries working to deploy and promote Facebook mobile products

20 Million Mobile Users



“..... Criminals go where people go.....”

10% of internet time is spent on social networking sites

Facebook is the 3<sup>rd</sup> biggest **country** in the world!

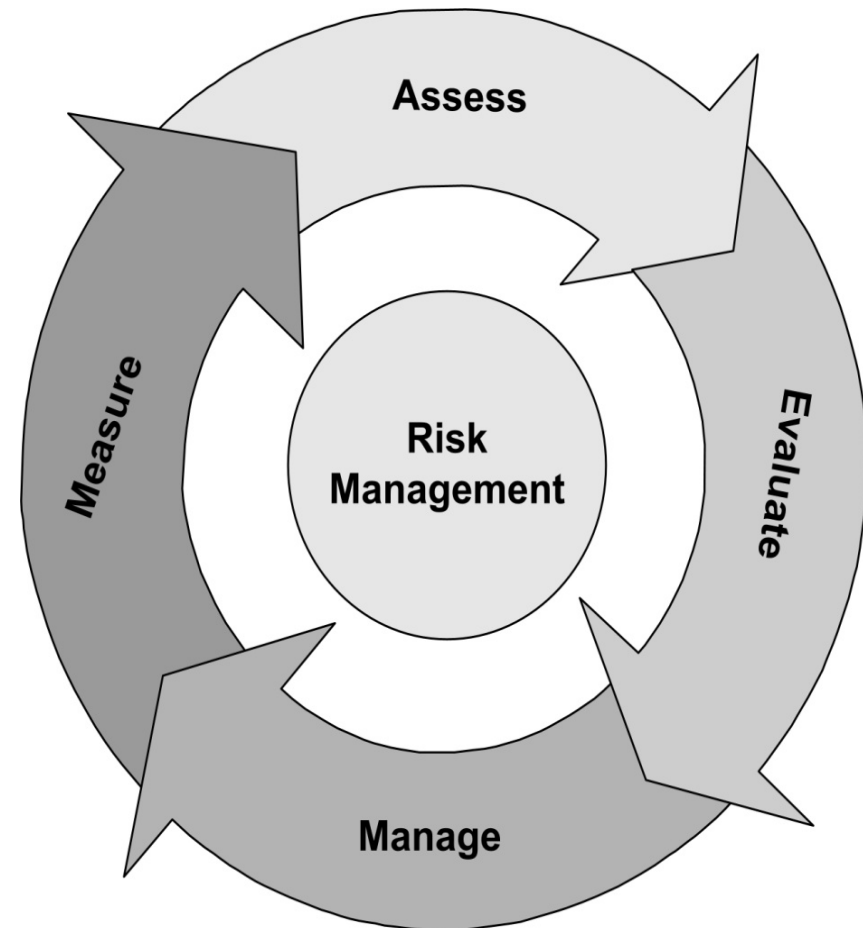


# CRO's and Cyber Threats

paul  dwyer  
SECURITY GRC & CYBER CRIME ADVISOR

**Automation:** Cybercriminals can automate mundane tasks - making denial of service attacks and large scale junk mail possible, just as they enable 100% surveillance of the Internet communications traffic of any organisation.

**Data collection:** digital data requires minimal storage space and is easier to harvest and manipulate



# CRO's and Cyber Threats

**Action at a distance:** in cyberspace, the criminal who is targeting your network may be based in Chechnya, Moldavia or on a Pacific island.

**Propagation:** the Web enables ideas, skills and digital tools to be shared around the world within hours. It also enables techniques to be widely replicated and a vast array of computers to be linked into any one attack.

These main characteristics mean that when the bad guys finds a weakness, they can exponentially exploit it within seconds from multiple jurisdictions. This is completely different from the “normal” type of risk that generally a CRO considers.



# Different Levels of Threat

**Low Hanging Fruit**

**Cyber Espionage**

**Targeted**

**Combination & “Low and Slow”**

**Major Players including Organised Crime**



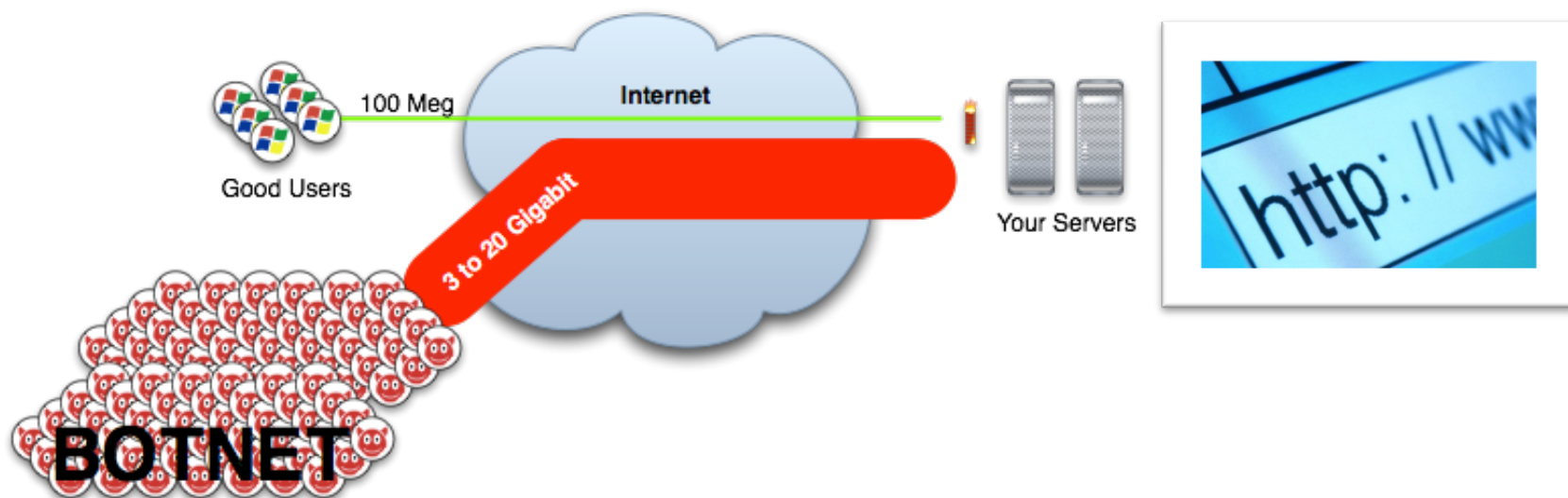
# How Easy is All This?

# How Easy is it to DDoS Someone?

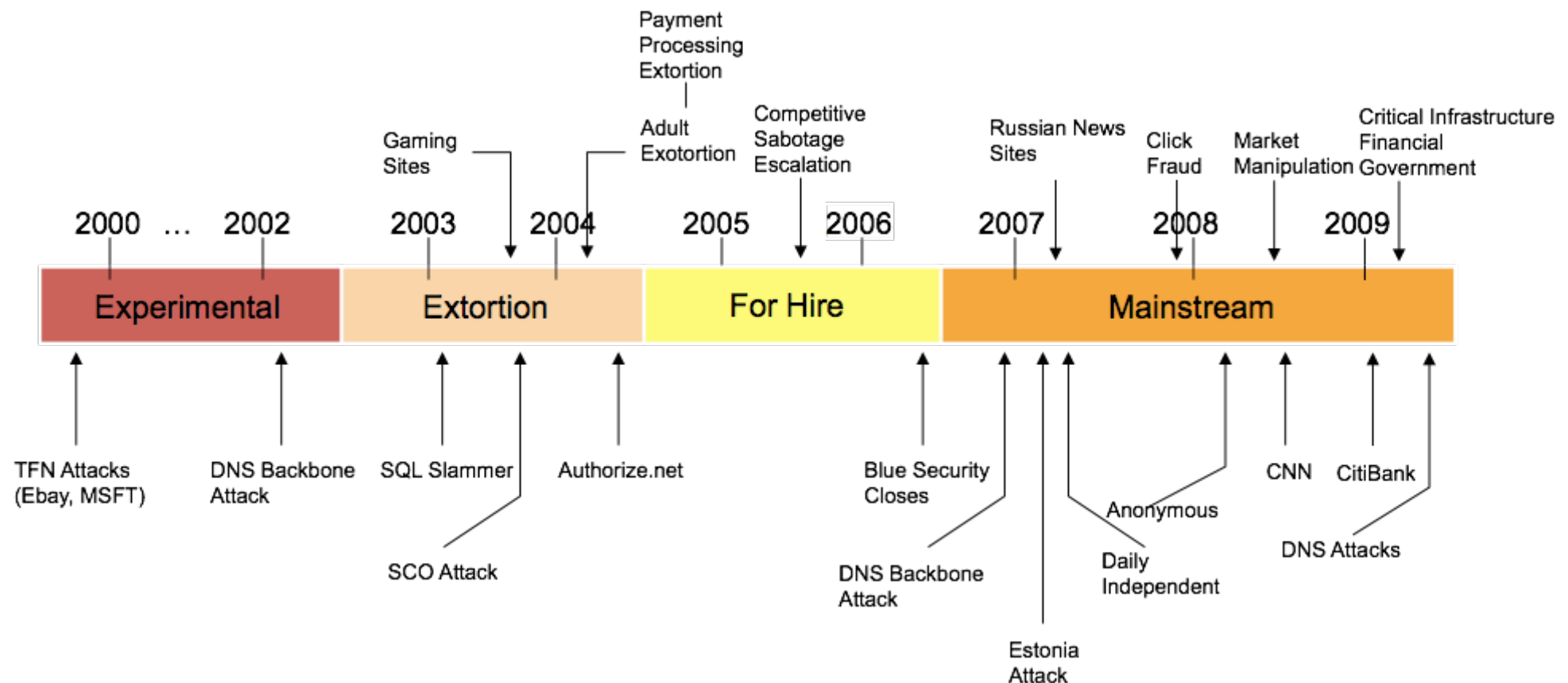


# What is a DDoS Attack

- An attempt to make a computer resource unavailable to users.
- Attacking computers are typically compromised PC's known as "Zombies". They attack simultaneously from many locations.
- Attacks come in many variations. These attacks continually evolve to outwit detection and mitigation devices.



# The Evolution of DDoS



DDoS is mainstream, and targeting the largest organisations and infrastructures

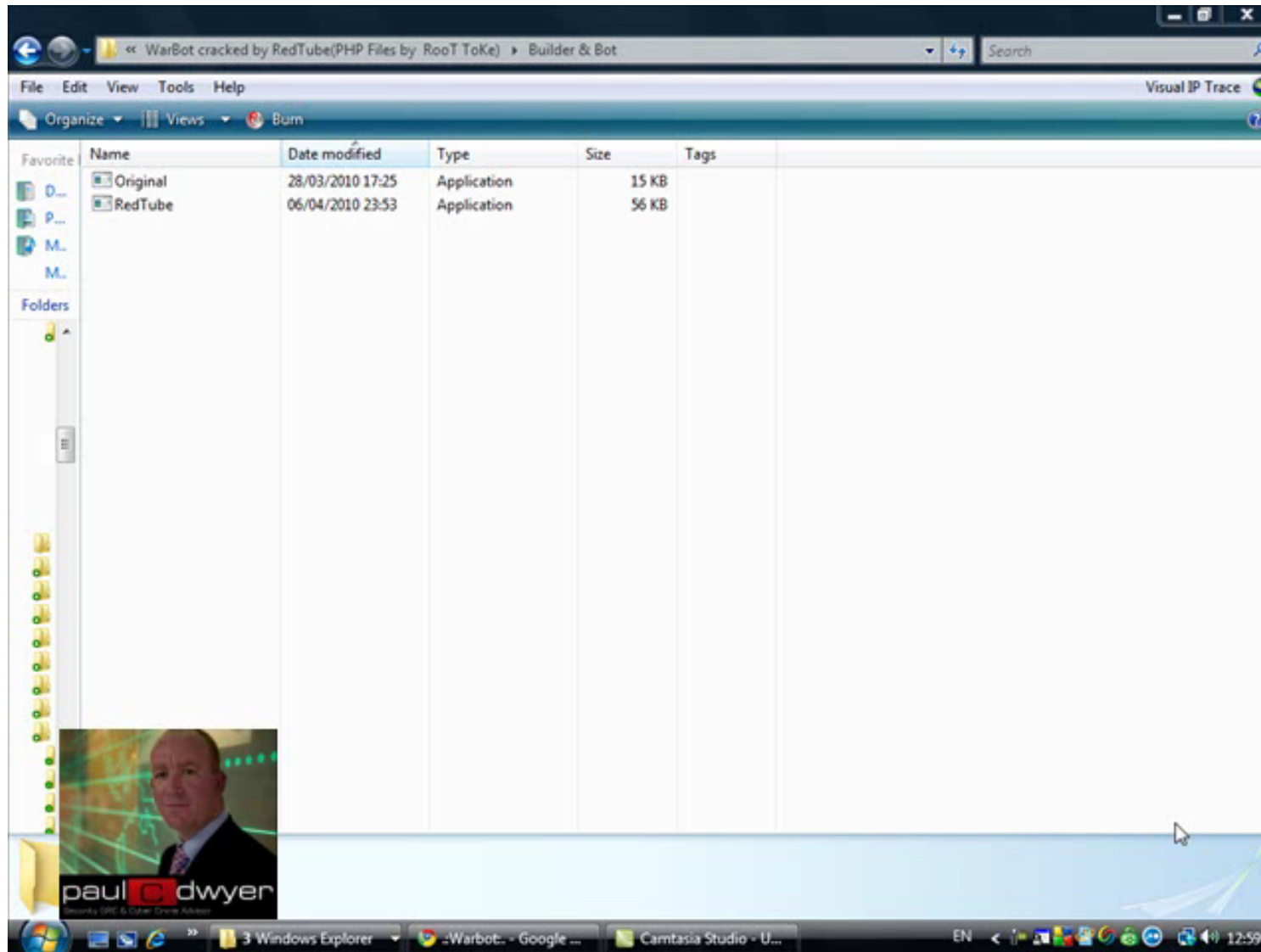
# As Easy As...

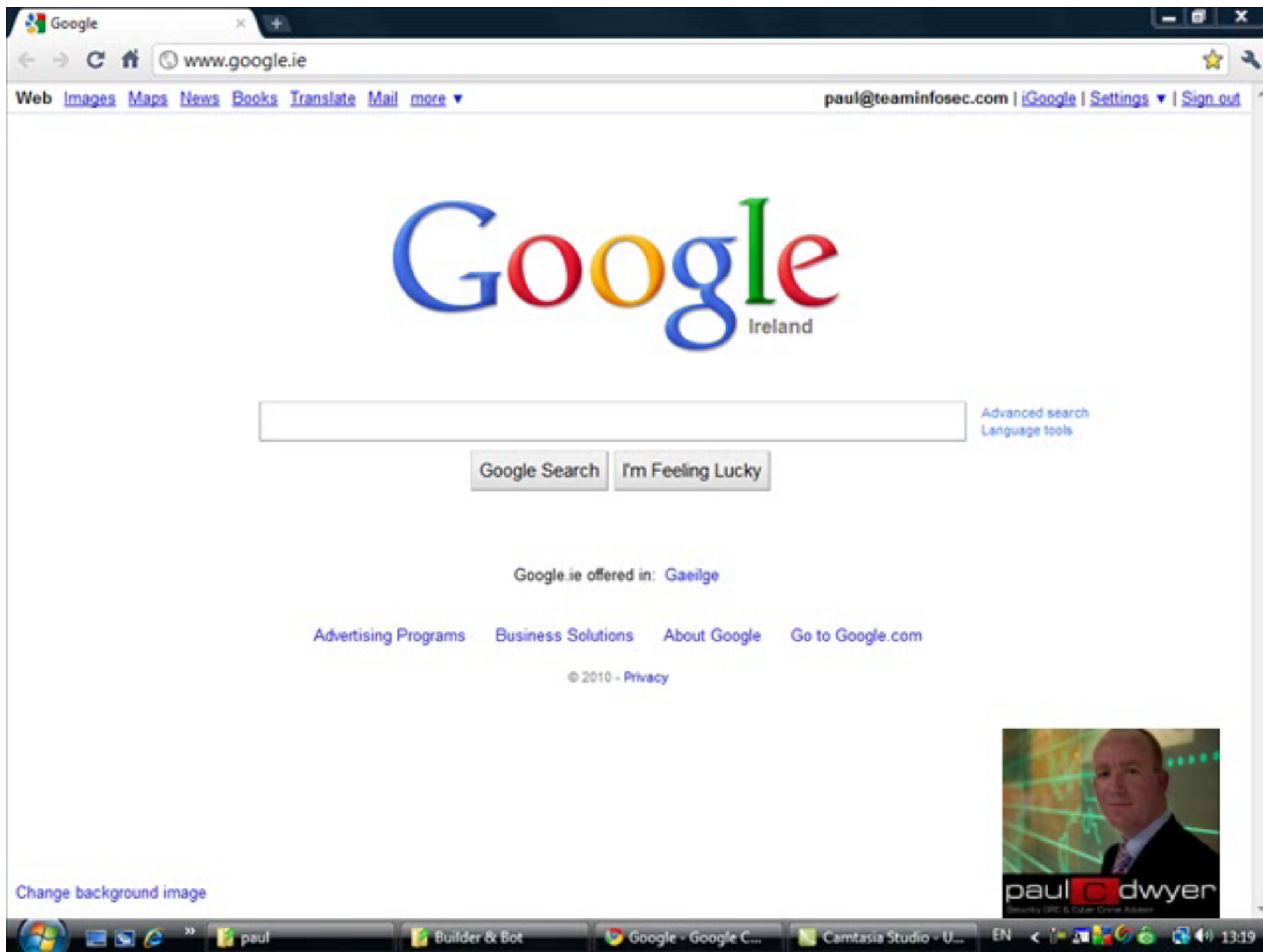
- 1) Search on Google and Youtube
- 2) Download Toolkit
- 3) Follow Instructions
  - a) Create Virus
  - b) Attack Site



# How Easy is a DDoS Attack

paul  dwyer  
SECURITY GRC & CYBER CRIME ADVISOR







# What's the Answer?

paul **C** dwyer  
SECURITY GRC & CYBER CRIME ADVISOR

## Attribution?



# Some Food for Thought

## Defence? More boxes

**Proactive Cyber Defence** means acting in anticipation to oppose an attack against computers and networks. It represents the dynamic between purely offensive and defensive action.

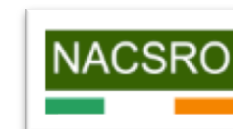
In the Fifth century, B.C., Sun Tzu (Art of War) advocated “**foreknowledge**” or predictive analysis as part of a winning strategy. He warned that planners must have a precise understanding of the active threat and not “**remain ignorant of the enemy’s condition.**”.

**Disruption? e.g. Phishing poisoning**

**Offensive? e.g. DDoS**

# Thank you

**paul C dwyer**  
SECURITY GRC & CYBER CRIME ADVISOR



[www.paulcdwyer.com](http://www.paulcdwyer.com)