Caa$:

Cybercrime as a Service

NATO OTAN

Berlin, May2015

Cpt. César Lorenzana

Cybercrime Central Unit

Guardia Civil (ES)

e©RIME ®EVOLUTION

- Romantic Lone Wolves (80´s - 2000)
- Cyber Crime Middle Age (2000 - 2004)
- Industrial Revolution (2004 - ??)

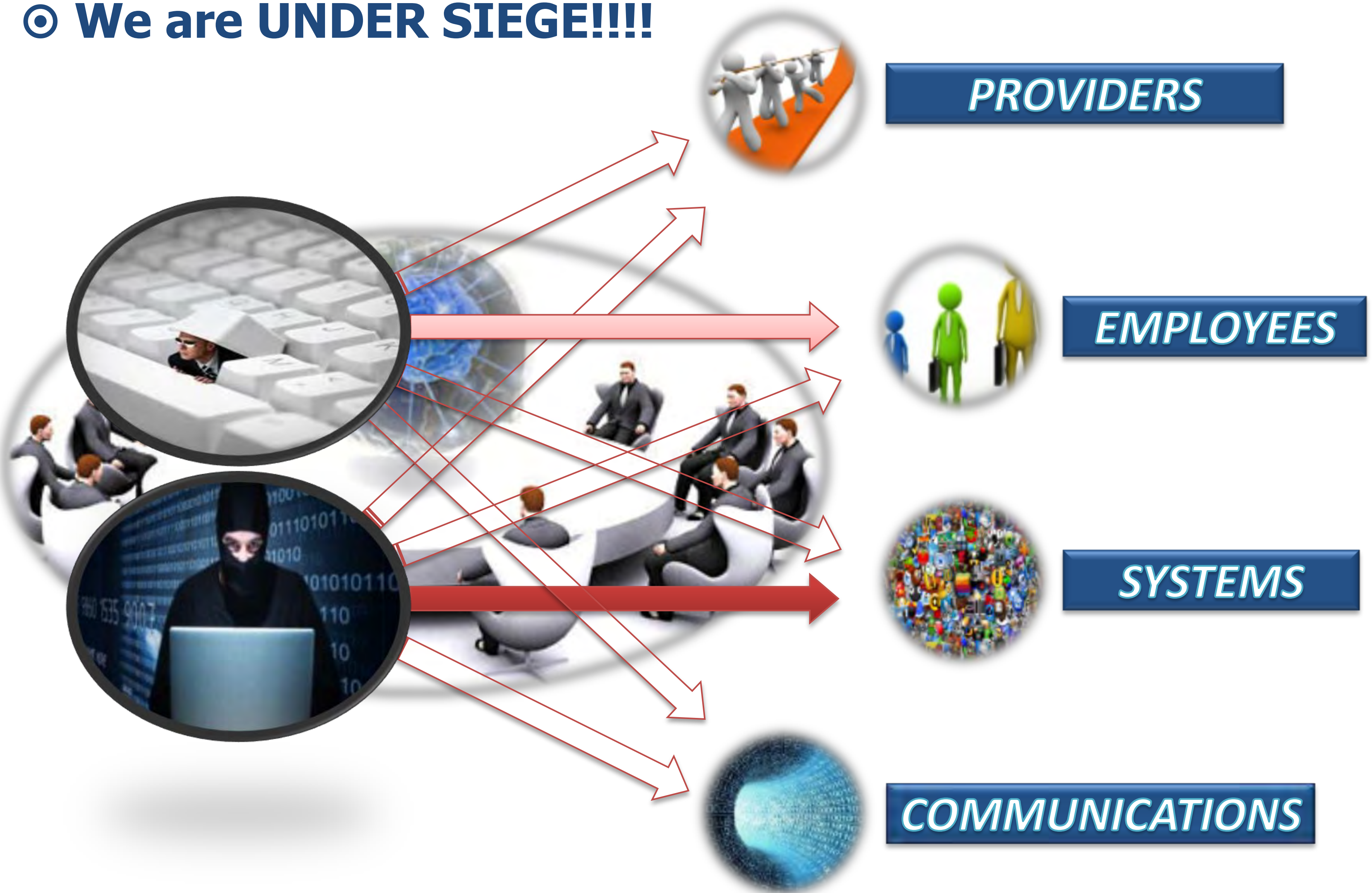
CYBERCRIME INDUSTRY

- Cybercrime Business Model
- Money Flow in Cybercrime

CRIMINAL SERVICES MARKET

- *RaaS - Research as a Service*
- *CaaS - Crimeware as a Service*
- *IaaS - Infrastructure as a Service*
- *HaaS - Hacking as a Service*

⊙ We are UNDER SIEGE!!!!


PROVIDERS

EMPLOYEES

SYSTEMS

COMMUNICATIONS

⊙ CyberAttacks vs. CyberEspionage

FUNDED BY ANYONE WILLING TO PAY FOR IT……ALWAYS BY PRO´s

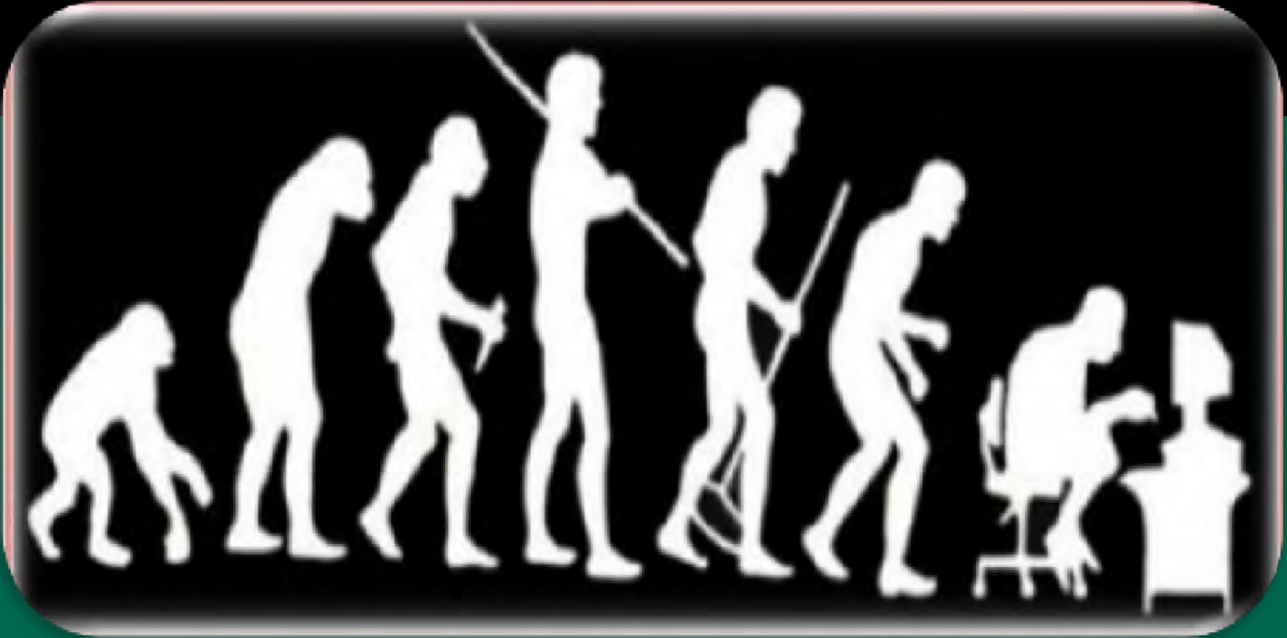
FOCUSED IN COMMERCIAL/BUSINESS TARGETS

REAL NEW ECONOMIC THREAT

FUNDED BY GOVERNMENTS……NOT ALWAYS EXECUTED BY THEM

FOCUSED IN STRATEGIC TARGETS

IT ALWAYS HAVE BEEN THERE….. NOW THEY USE IT



HOW IT ALL STARTED?

Hackers First Generation - Lone Wolf

Kevin Mitnick
January 21, 1995
Compromised, DEC, IBM, HP, Motorola, PacBell, NEC, ….

Chen Ing-Hau, 24, Taiwan
Arrested September 15, 2000
CIH (Chernobyl) Virus

Jeffrey Lee Parson, 18, USA
Arrested August 29, 2003
Blaster Worm ('B' variants only), DDoS

Sven Jaschan, 18, Germany
Arrested May 7, 2004
NetSky (Sasser) Worm

Cyber Criminals - "Proof of Concept" for making $

Farid Essebar, 18, Morocco
Arrested August 25, 2005
Mytob and Zotob (Bozori) Worms

Atilla Ekici, 21, Turkey
Arrested August 25, 2005
Operating Mytob and Zotob botnets

Jeanson James Ancheta, 24, USA
Arrested November 3, 2005
Rxbot zombie networks for hire (spam and DDoS)

Cyber Crime Goes Big Time

- London branch of Japan's Sumitomo Mitsui Bank
- Worked with insiders through Aharon Abu-Hamra, a 35-year-old Tel Aviv resident
- Injected a Trojan to gather credentials to a transfer system
- Attempted to transfer £220 million into accounts he controlled around the world
- £13.9 million to his own business account

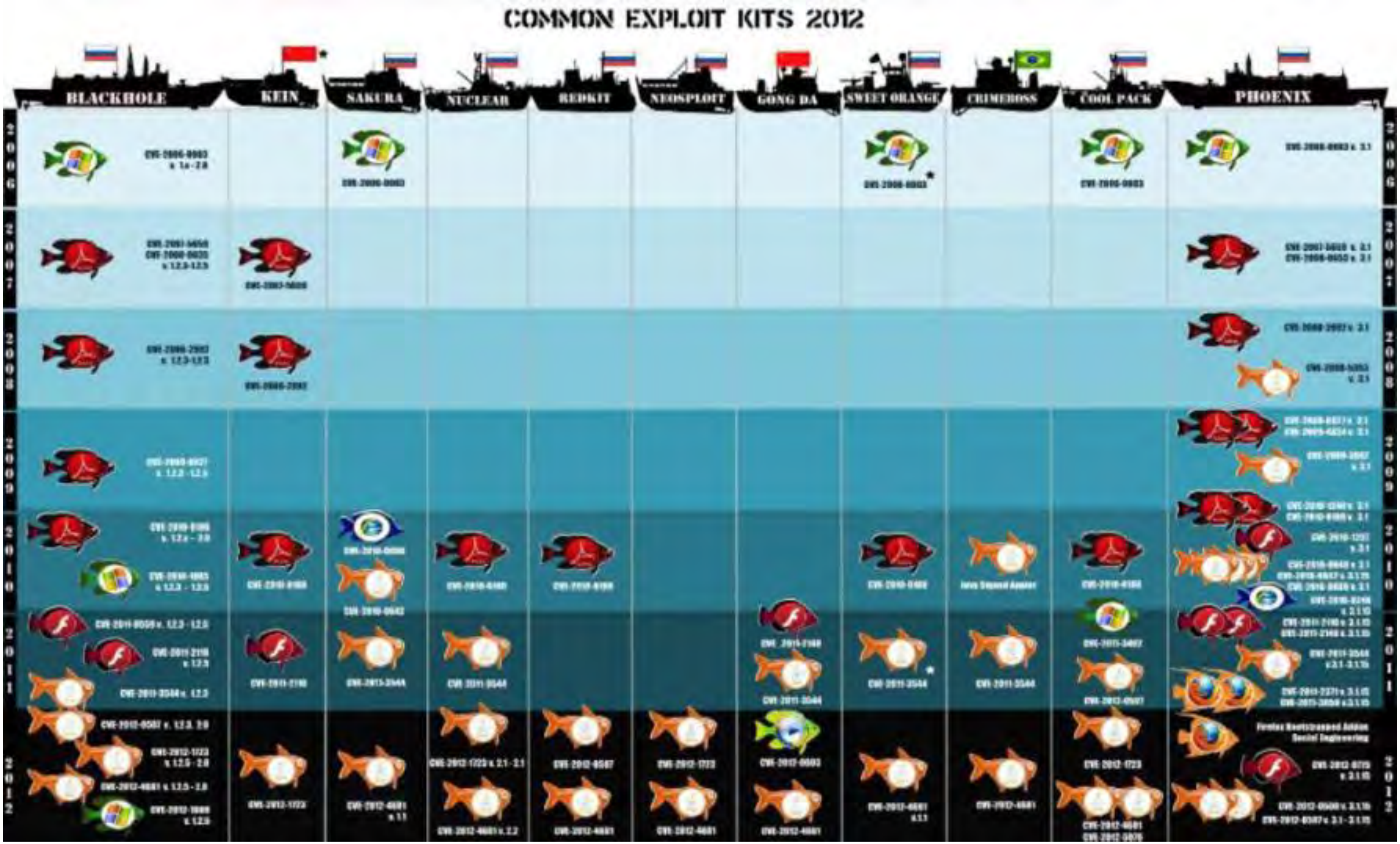
Yaron Bolondi, 32, Israel
Arrested March 16, 2005

Albert Gonzalez – Segvec, Soupnazi, J4guar

- Indicted on Aug 17, 2009
- Stole 130,000,000 credit card numbers
- Worked out of Miami – his one flaw
- Worked as an **international organized cybercrime group**
  - 3 in the Ukraine
    - Including Maksik who earned of $11m between 2004-2006
  - 2 in China
  - 1 from Belarus
  - 1 from Estonia
  - 1 from unknown location that goes by “Delperiao”

INDUSTRIAL REVOLUTION !!!!!!

- ORGANIZED TEAMS / “”NEW PLAYERS”
- SPECIALIZE & DIVERSIFY ACTIVITIES
- NEW BUSSINESS MODEL
- NEW TARGETS (SCADA & CONTROL SYSTEMS)
- SOPHISTICATED & AGGRESSIVE

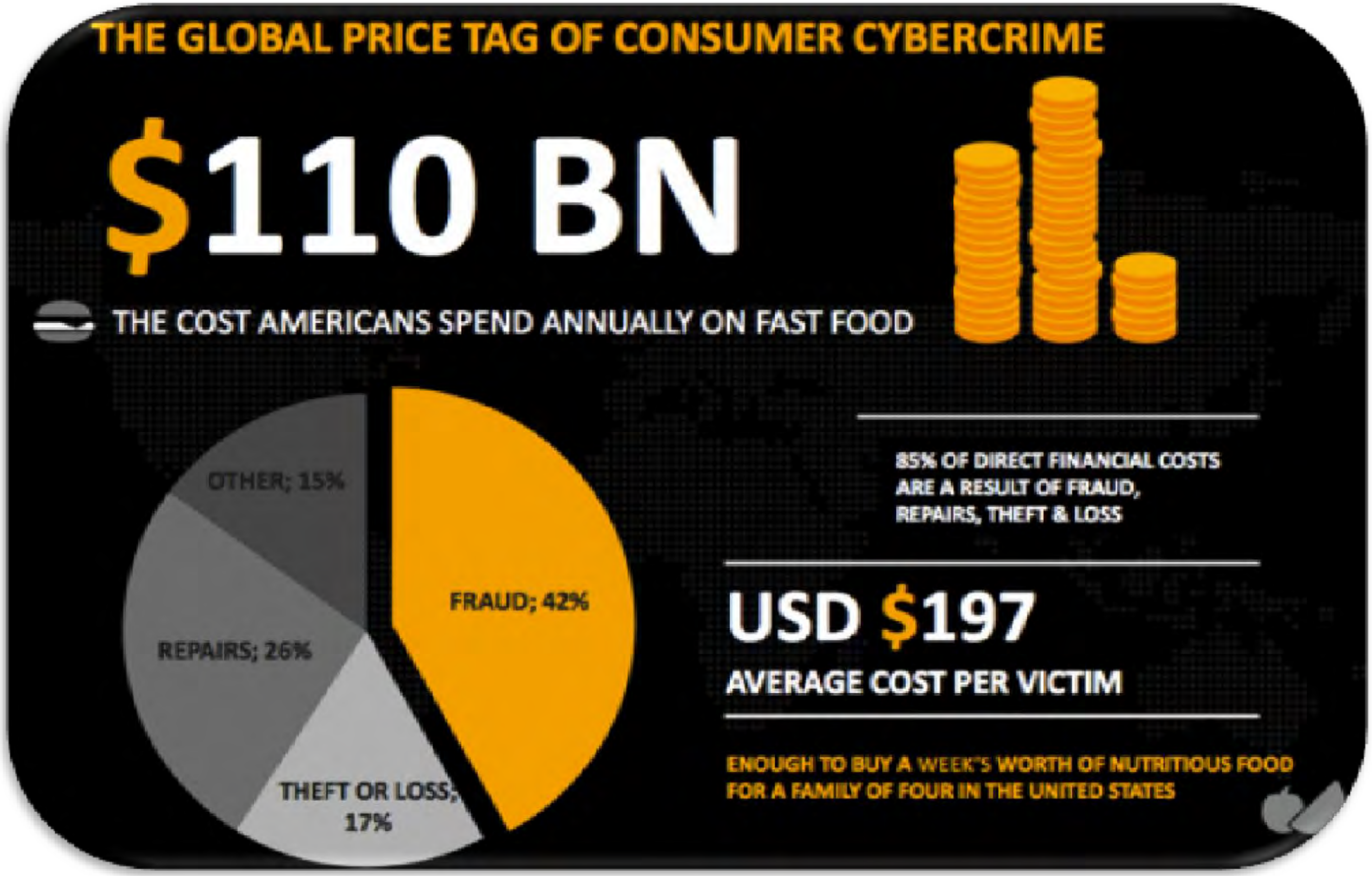

COMMON EXPLOIT KITS 2012
BLACKHOLE
KEIN
SAKURA
NUCLEAR
REDKIT
NEOSPLOIT
GONG DA
SWEET ORANGE
CRIMEBOSS
COOL PACK
PHOENIX
2006
2007
2008
2009
2010
2011
2012
Java Signed Applet
Firefox Bootstrapped Addon
Social Engineering

Driving Factors Behind Cyber Crime

Picture provided by "energizer" hacking group
90 day project take
$300,000 - $500,000

- Profitable
- Low risk
- New services to exploit
- Easy (technically)
- Easy (morally – you never meet the victim)

CYBERCRIME INDUSTRY



THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME

$110 BN

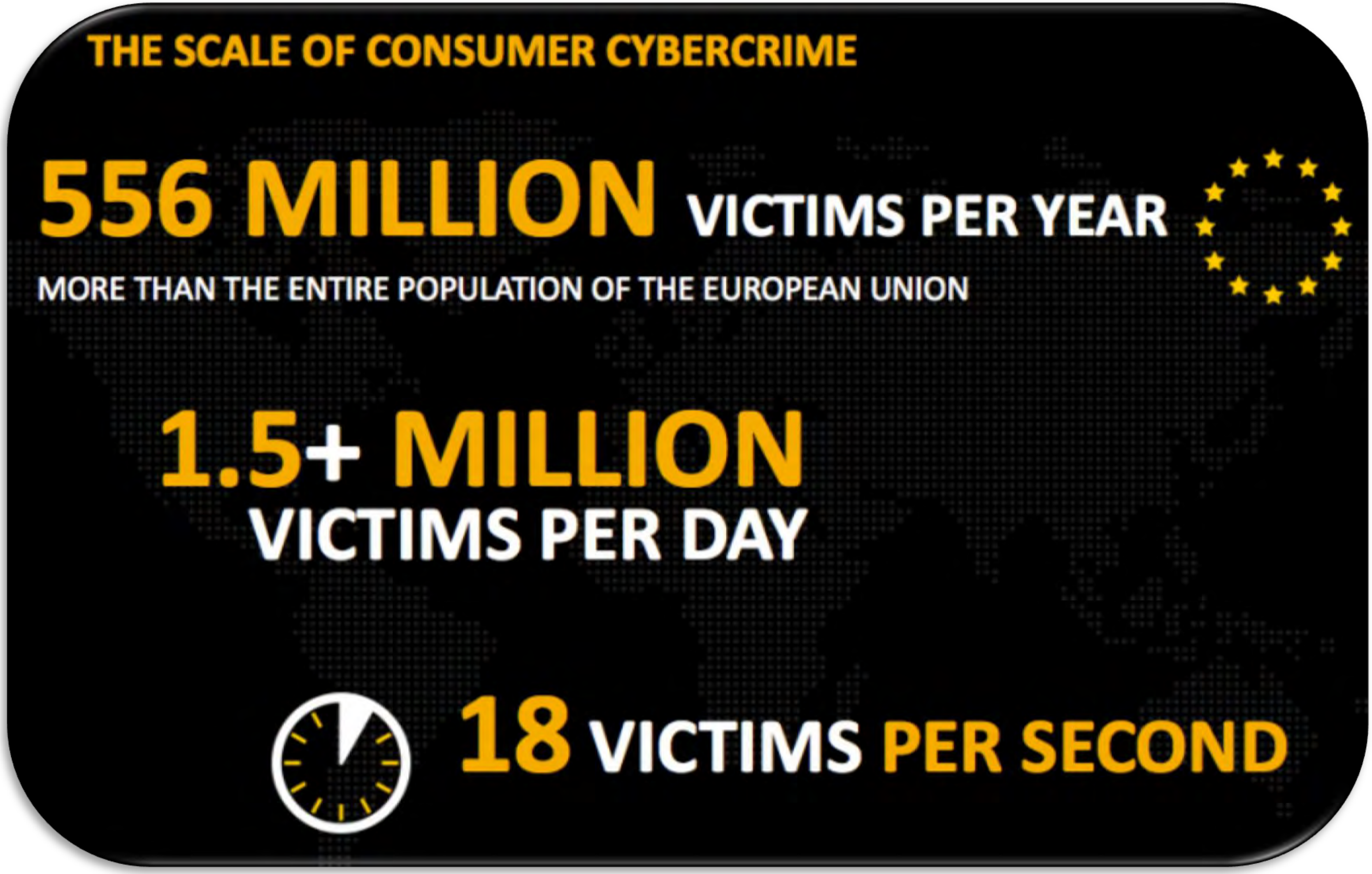
THE COST AMERICANS SPEND ANNUALLY ON FAST FOOD

85% OF DIRECT FINANCIAL COSTS ARE A RESULT OF FRAUD, REPAIRS, THEFT & LOSS

USD $197

AVERAGE COST PER VICTIM

ENOUGH TO BUY A WEEK'S WORTH OF NUTRITIOUS FOOD FOR A FAMILY OF FOUR IN THE UNITED STATES



THE SCALE OF CONSUMER CYBERCRIME

556 MILLION VICTIMS PER YEAR

MORE THAN THE ENTIRE POPULATION OF THE EUROPEAN UNION

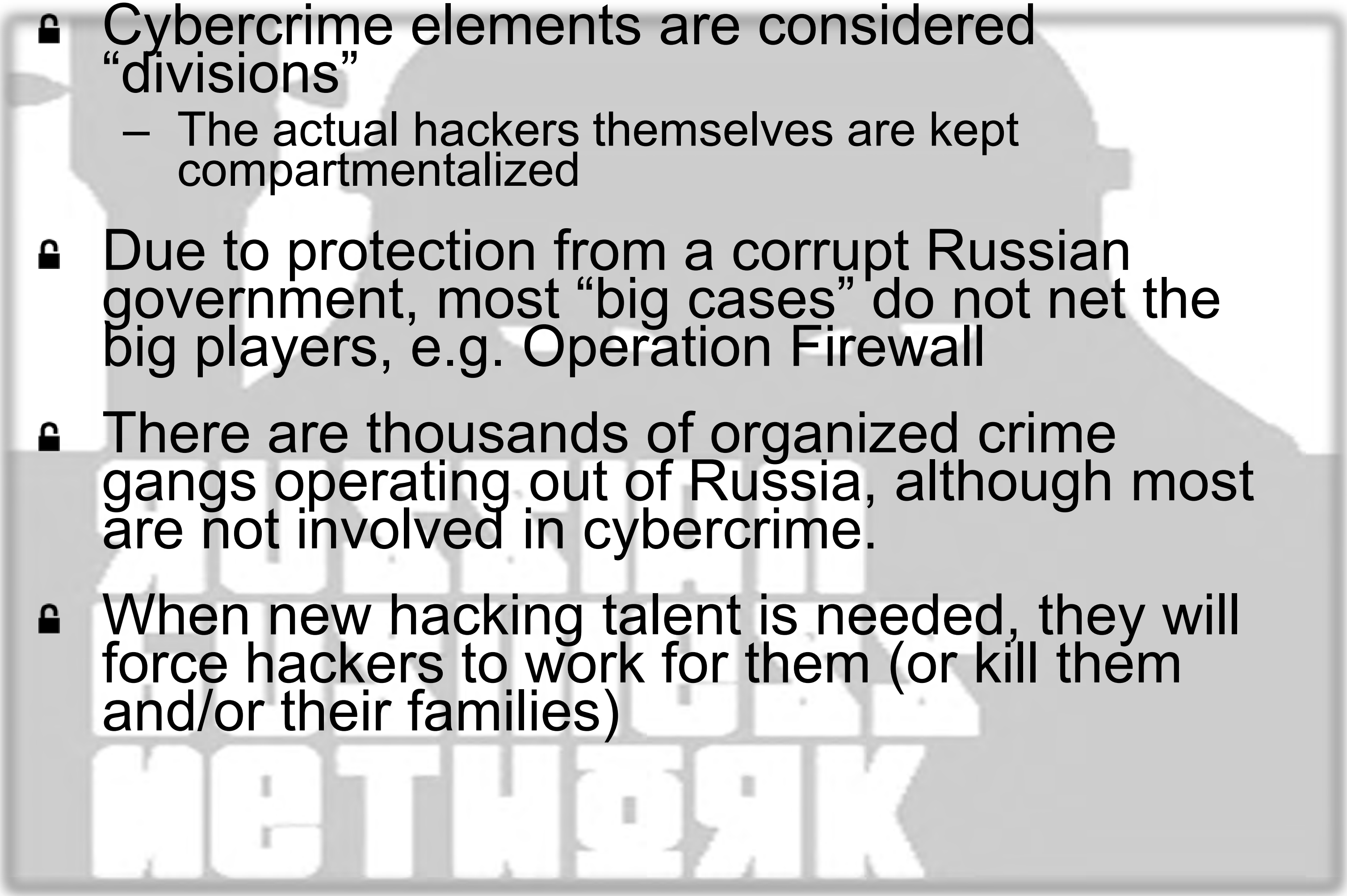
1.5+ MILLION VICTIMS PER DAY

18 VICTIMS PER SECOND

The Players

- Russian Business Network (Mafia)
- Professional Hackers
- Basic Cybercrime Organizations

Russian Business Network (Mafia)



- Cybercrime elements are considered “divisions”
  - The actual hackers themselves are kept compartmentalized
- Due to protection from a corrupt Russian government, most “big cases” do not net the big players, e.g. Operation Firewall
- There are thousands of organized crime gangs operating out of Russia, although most are not involved in cybercrime.
- When new hacking talent is needed, they will force hackers to work for them (or kill them and/or their families)

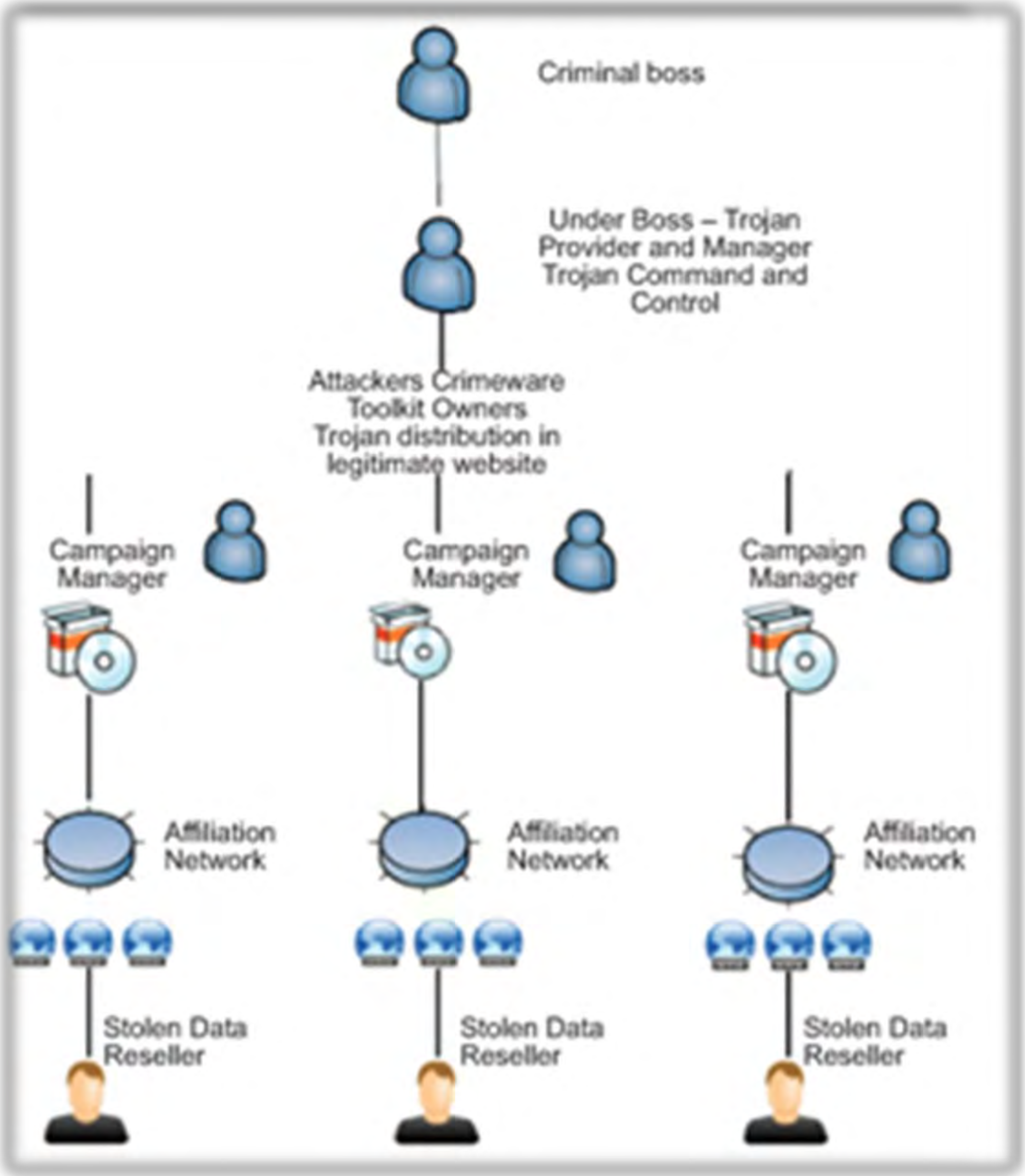
Professional Hackers

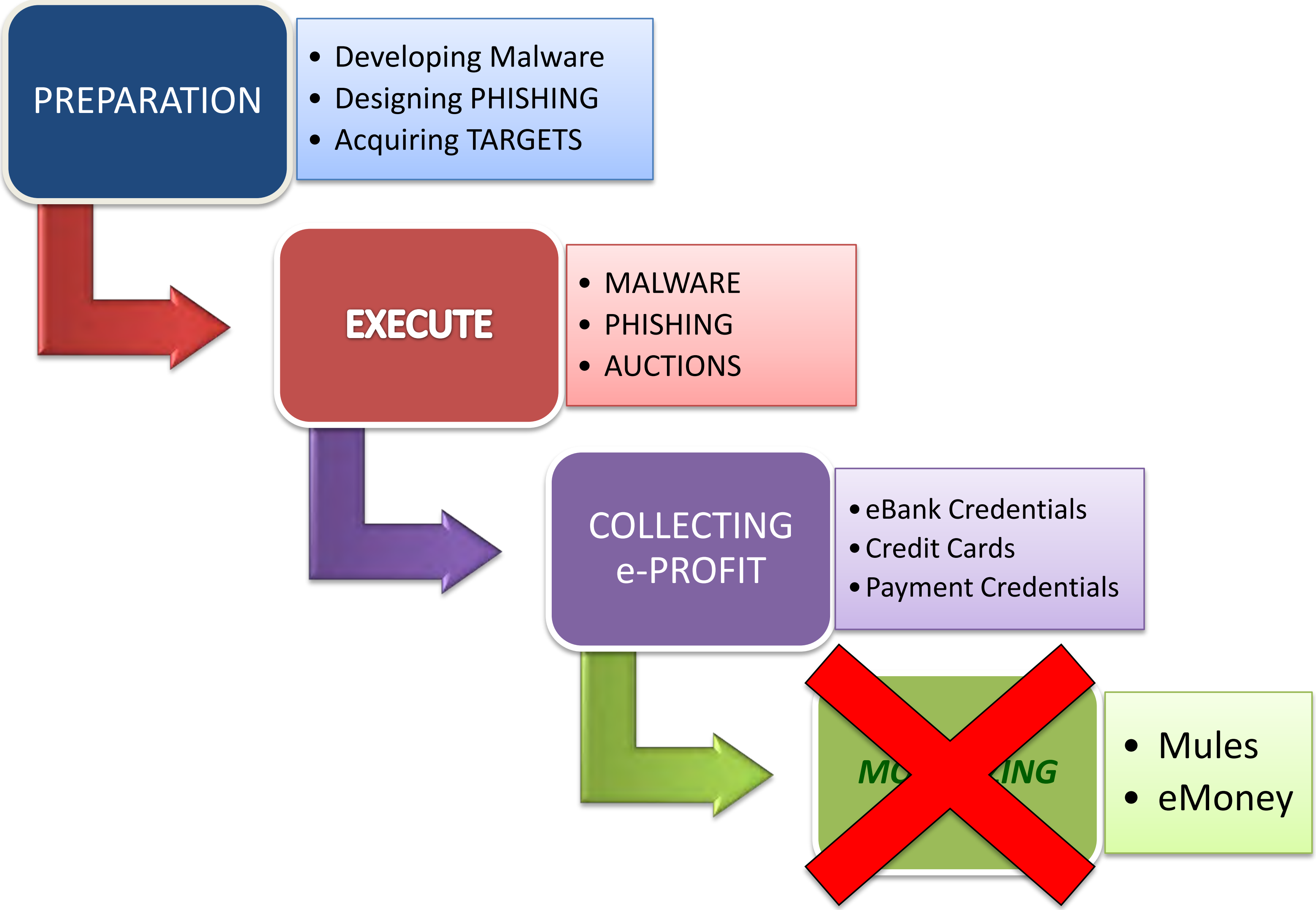
- Paid per the job, usually flat rates
- State-side hackers may earn up to $200K a year
- The work is usually writing tools for others to use, developing/finding new exploits, and coding up malware
- Occasionally they will do a black bag job, but these are rare, unless they are simply looking for “loot” on easy targets

Basic Cybercrime Organizations

- Fluid and change members frequently
- Will form and disband on a “per project” basis
- Rife with amateurs, take a lot of risk considering the small payoffs
- Although the most troublesome, they are considered the bottom feeders
  - Think criminal script kiddies
  - This is usually who the Feds get, not the big guys

Caa$: Cybercrime as a Service





PREPARATION

- Developing Malware
- Designing PHISHING
- Acquiring TARGETS

EXECUTE

- MALWARE
- PHISHING
- AUCTIONS

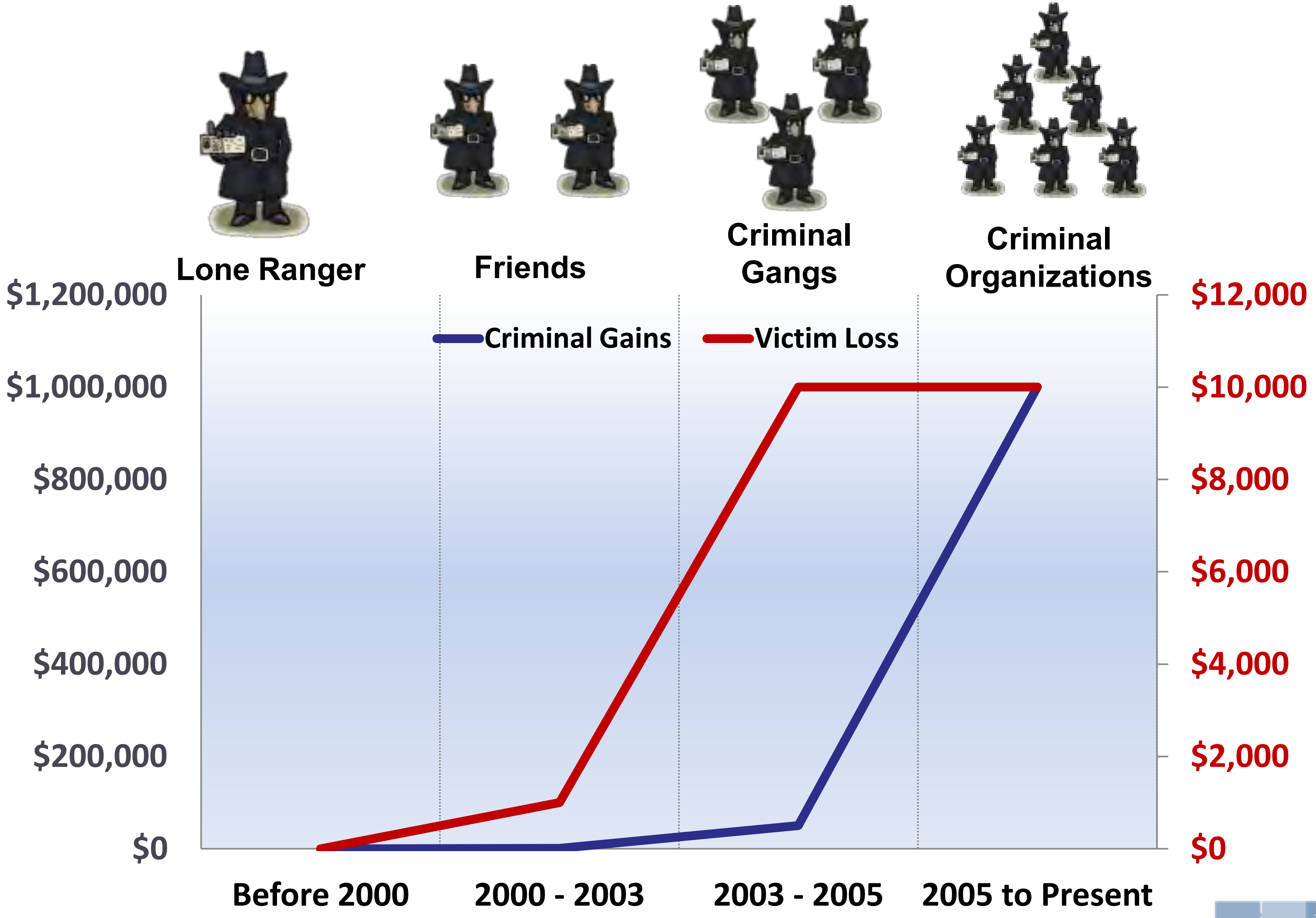
COLLECTING e-PROFIT

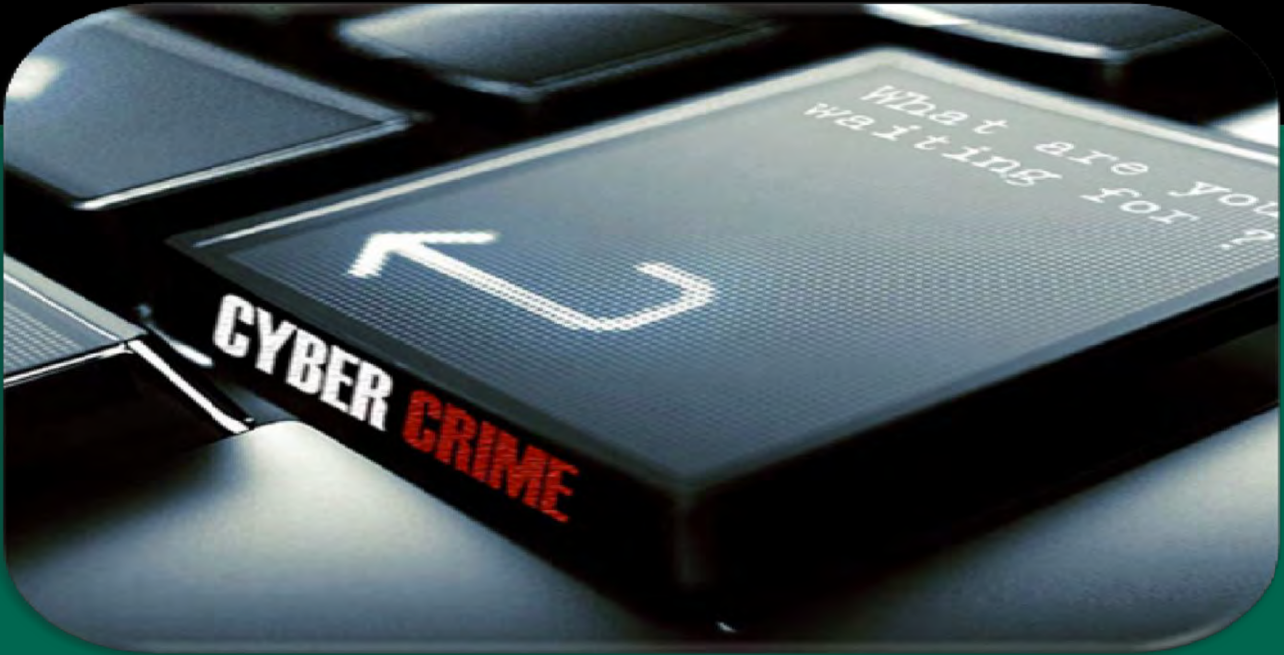
- eBank Credentials
- Credit Cards
- Payment Credentials

MO ING

- Mules
- eMoney

Cyber Crime Trends





CRIMINAL SERVICES MARKET

Internet Black Market Pricing Guide

- Exploit code for known flaw - $100-$500 if no exploit code exists
  - Price drops to $0 after exploit code is "public"
- Exploit code for unknown flaw - $1000-$5000
  - Buyers include iDefense, Russian Mafia, Chinese and French governments, etc
- List of 5000 IP addresses of computers infected with spyware/trojan for remote control - $150-$500
- List of 1000 working credit card numbers - $500-$5000
- Annual salary of a top-end skilled black hat hacker working for spammers - $100K-$200K

More details on:

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf

Caa$: Cybercrime as a Service

Resear

- doesn´t have t sources
- commercial co sale of zero-
- individuals w

a Service

- loits used for the
- alware
- nto physical

Cybercrime as a Service Caa$

- multitude of services
- deep technical expertise is not a prerequisite.
- the services-based allows hiring individuals to undertake specific tasks
- broad variety of products and services available to buy or rent

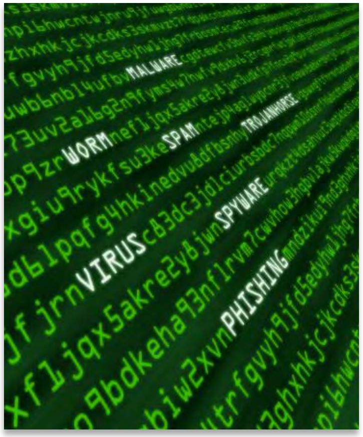
Infraestru

- delivering their victims
- rental of a network of computers
- availability bullet-proof hosting

Service

- of an attack
- outsourcing of the attack entirely
- availability of information

Research as a Service - RaaS



- *Vulnerabilities for sale: a commercial marketplace*
- *Exploit Brokers*
- *Spam email DB´s*

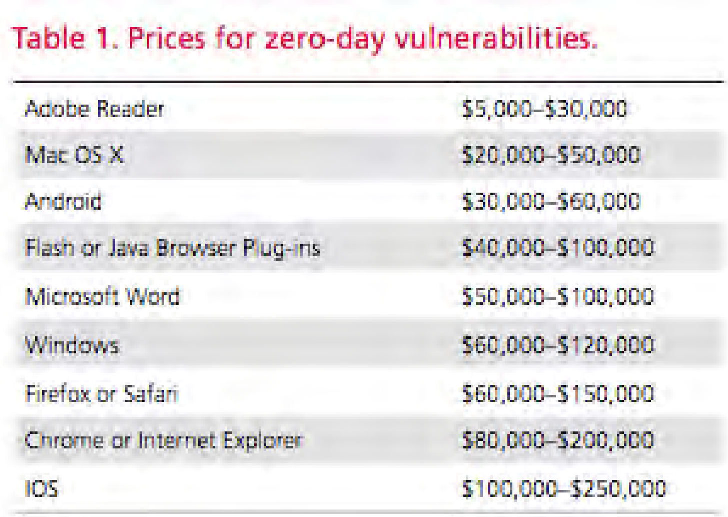
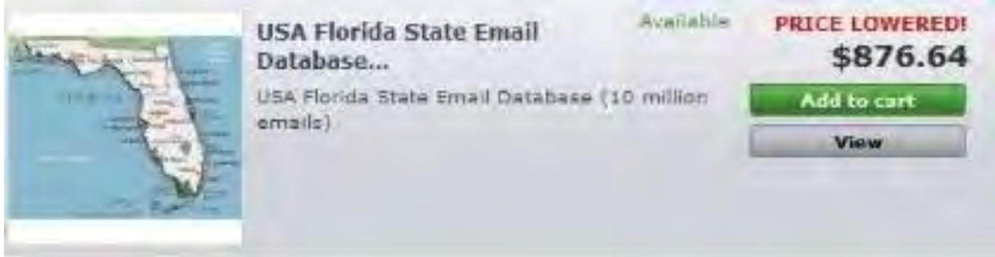


Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Microsoft Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

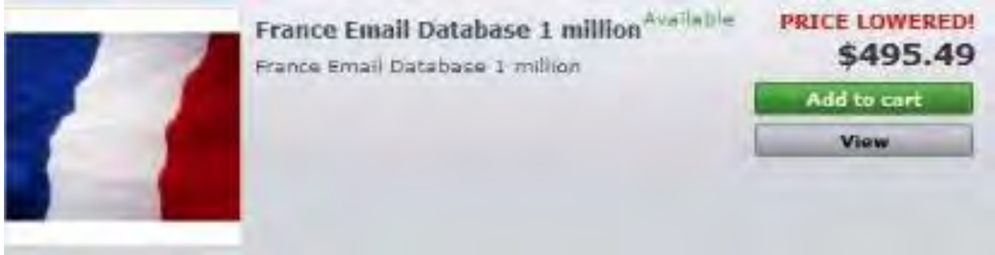


USA Florida State Email Database...

Available

PRICE LOWERED!
$876.64

USA Florida State Email Database (10 million emails)



France Email Database 1 million

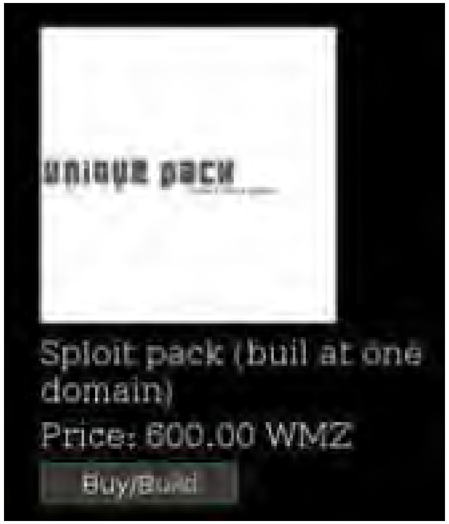
Available

PRICE LOWERED!
$495.49

France Email Database 1 million

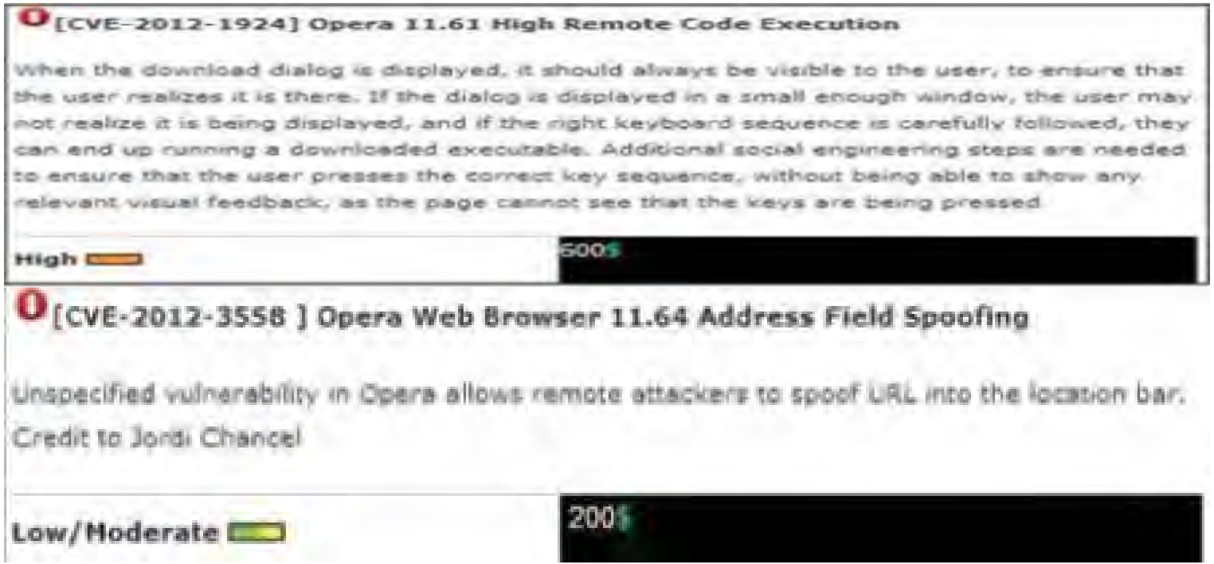
Crimeware as a Service - CaaS

- *Professional Services*
- *Malware Services (Rootkit & Ransomware Services)*
- *Exploits & Crypters Development*
- *Check AV Detection Rate*



Sploit pack (buil at one domain)

Price: 600.00 WMZ



[CVE-2012-1924] Opera 11.61 High Remote Code Execution

When the download dialog is displayed, it should always be visible to the user, to ensure that the user realizes it is there. If the dialog is displayed in a small enough window, the user may not realize it is being displayed, and if the right keyboard sequence is carefully followed, they can end up running a downloaded executable. Additional social engineering steps are needed to ensure that the user presses the correct key sequence, without being able to show any relevant visual feedback, as the page cannot see that the keys are being pressed

High 🟧 600$

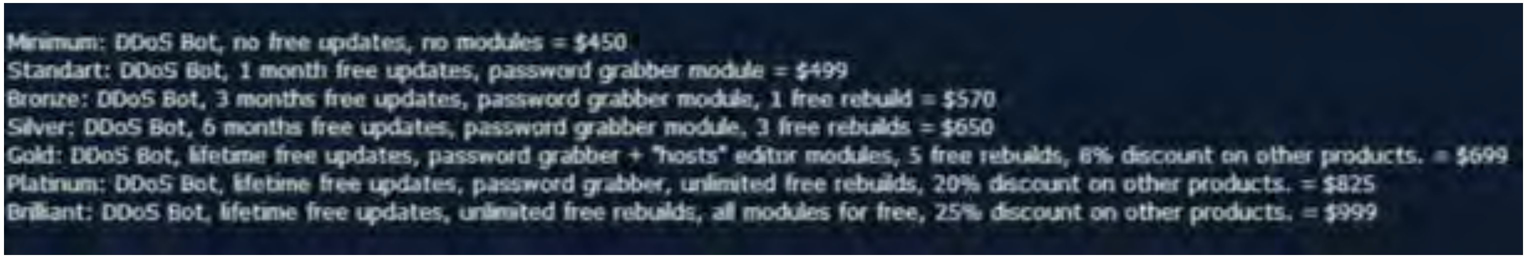
[CVE-2012-3558] Opera Web Browser 11.64 Address Field Spoofing

Unspecified vulnerability in Opera allows remote attackers to spoof URL into the location bar. Credit to Jordi Chancel

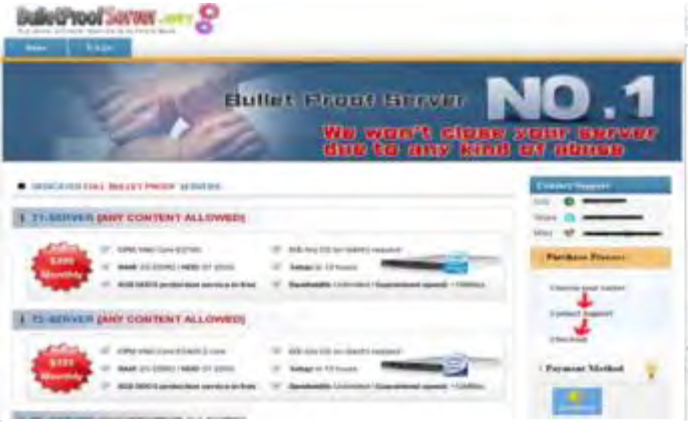
Low/Moderate 🟩 200$

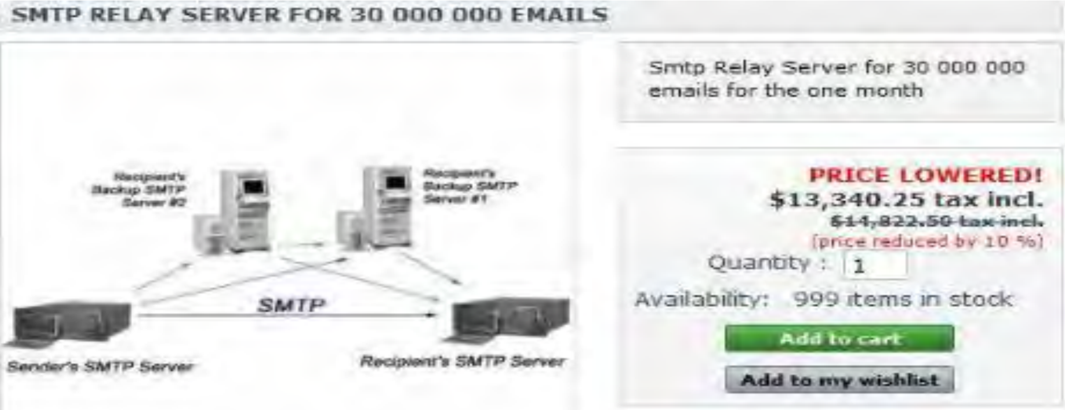
Infrastructure as a Service - IaaS

- ***BotNets***
- ***Hosting Services (Bulletproof Hosters)***
- ***Spam Services***



Minimum: DDoS Bot, no free updates, no modules = $450
Standart: DDoS Bot, 1 month free updates, password grabber module = $499
Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = $570
Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = $650
Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = $699
Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = $825
Brillant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = $999


BulletProofServer
Bullet Proof Server NO.1
We won't close your server due to any kind of abuse
T1-SERVER (ANY CONTENT ALLOWED)
T2-SERVER (ANY CONTENT ALLOWED)
Contact Support
Purchase Process
Payment Method



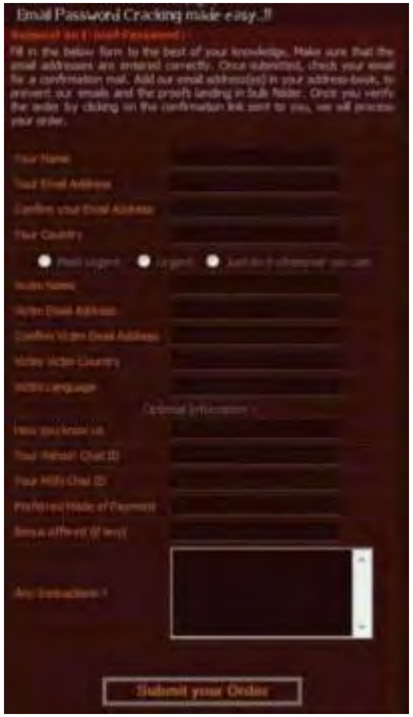
SMTP RELAY SERVER FOR 30 000 000 EMAILS

Smtp Relay Server for 30 000 000 emails for the one month

PRICE LOWERED!
$13,340.25 tax incl.
~~$14,822.50 tax incl.~~
(price reduced by 10 %)
Quantity : 1
Availability: 999 items in stock

Hacking as a Service - HaaS

- *Password Cracking Services*
- *Denial of Service (DDoS)*
- *Credit Card DB´s*
- *Login Credentials*



Email Password Cracking made easy..!!

[illegible]

Fill in the below form to the best of your knowledge. Make sure that the email addresses are entered correctly. Once submitted, check your email for a confirmation mail. Add our email address(es) in your address-book, to prevent our emails and the proofs landing in bulk folder. Once you verify the order by clicking on the confirmation link sent to you, we will process your order.

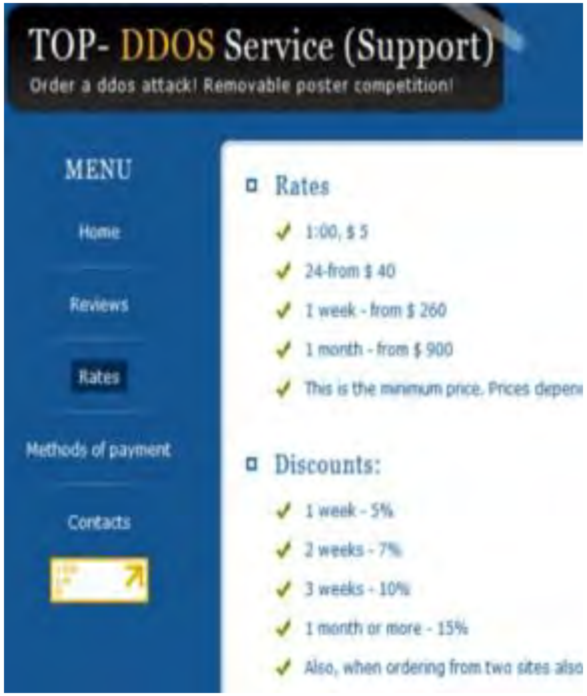
Your Name	
Your Email Address	
Confirm your Email Address	
Your Country	

○ Most Urgent ○ Urgent ○ Just do it whenever you can

Victim Name	
Victim Email Address	
Confirm Victim Email Address	
Victim Victim Country	
Victim Language	

Optional Information :

How you know us	
Your Yahoo! Chat ID	
Your MSN Chat ID	
Preferred Mode of Payment	
Bonus offered (if any)	
Any Instructions ?	



TOP- DDOS Service (Support)

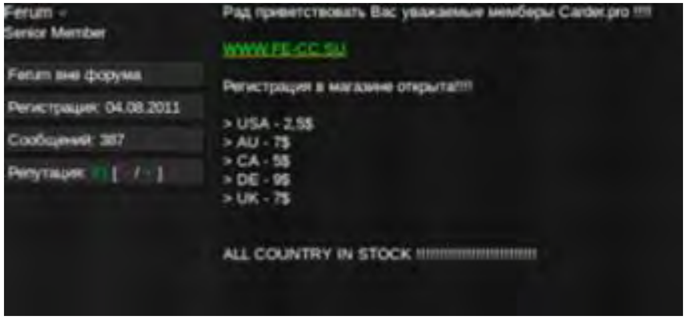
Order a ddos attack! Removable poster competition!

Rates

- ✓ 1:00, $ 5
- ✓ 24-from $ 40
- ✓ 1 week - from $ 260
- ✓ 1 month - from $ 900
- ✓ This is the minimum price. Prices depen

Discounts:

- ✓ 1 week - 5%
- ✓ 2 weeks - 7%
- ✓ 3 weeks - 10%
- ✓ 1 month or more - 15%
- ✓ Also, when ordering from two sites also



Ferum -
Senior Member

Ferum вне форума
Регистрация: 04.08.2011
Сообщений: 387
Репутация: [illegible]

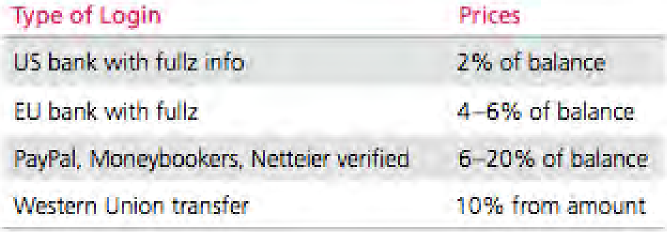
Рад приветствовать Вас уважаемые мемберы Carder.pro !!!!

WWW.FE-CC.SU

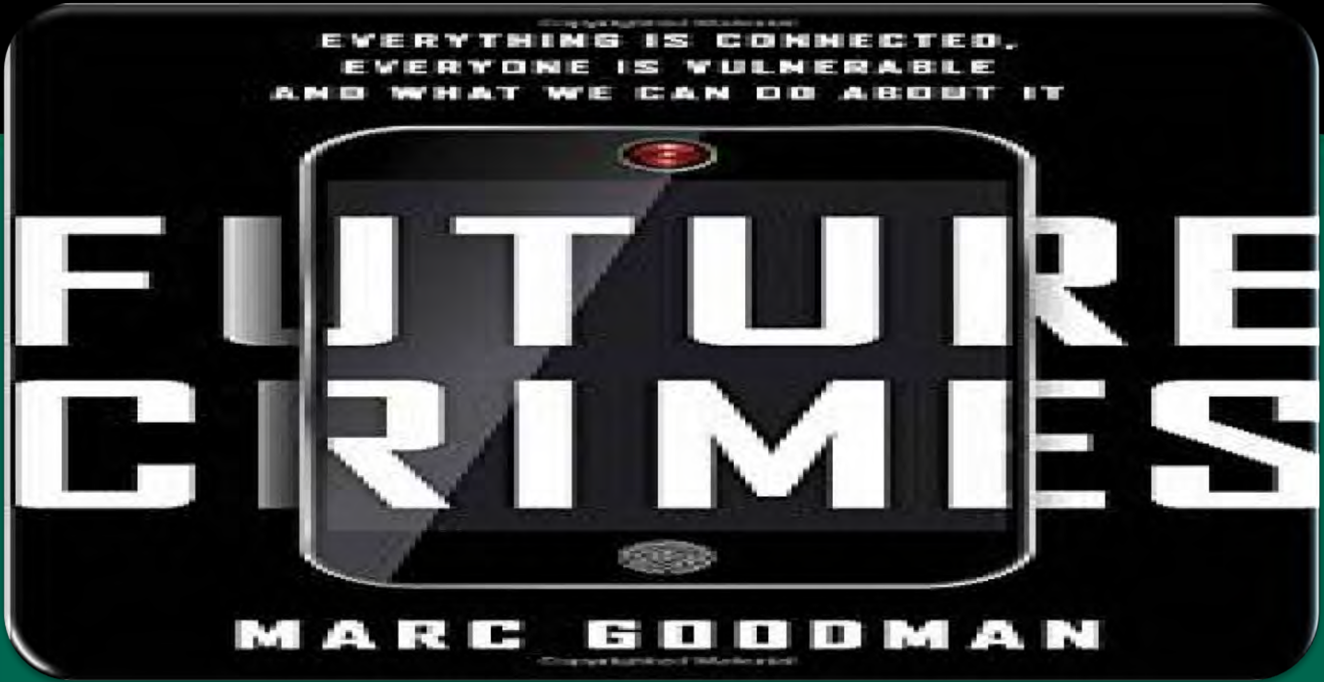
Регистрация в магазине открыта!!!!

> USA - 2.5$
> AU - 7$
> CA - 5$
> DE - 9$
> UK - 7$

ALL COUNTRY IN STOCK !!!!!!!!!!!!!!!!!!!!!!!!!

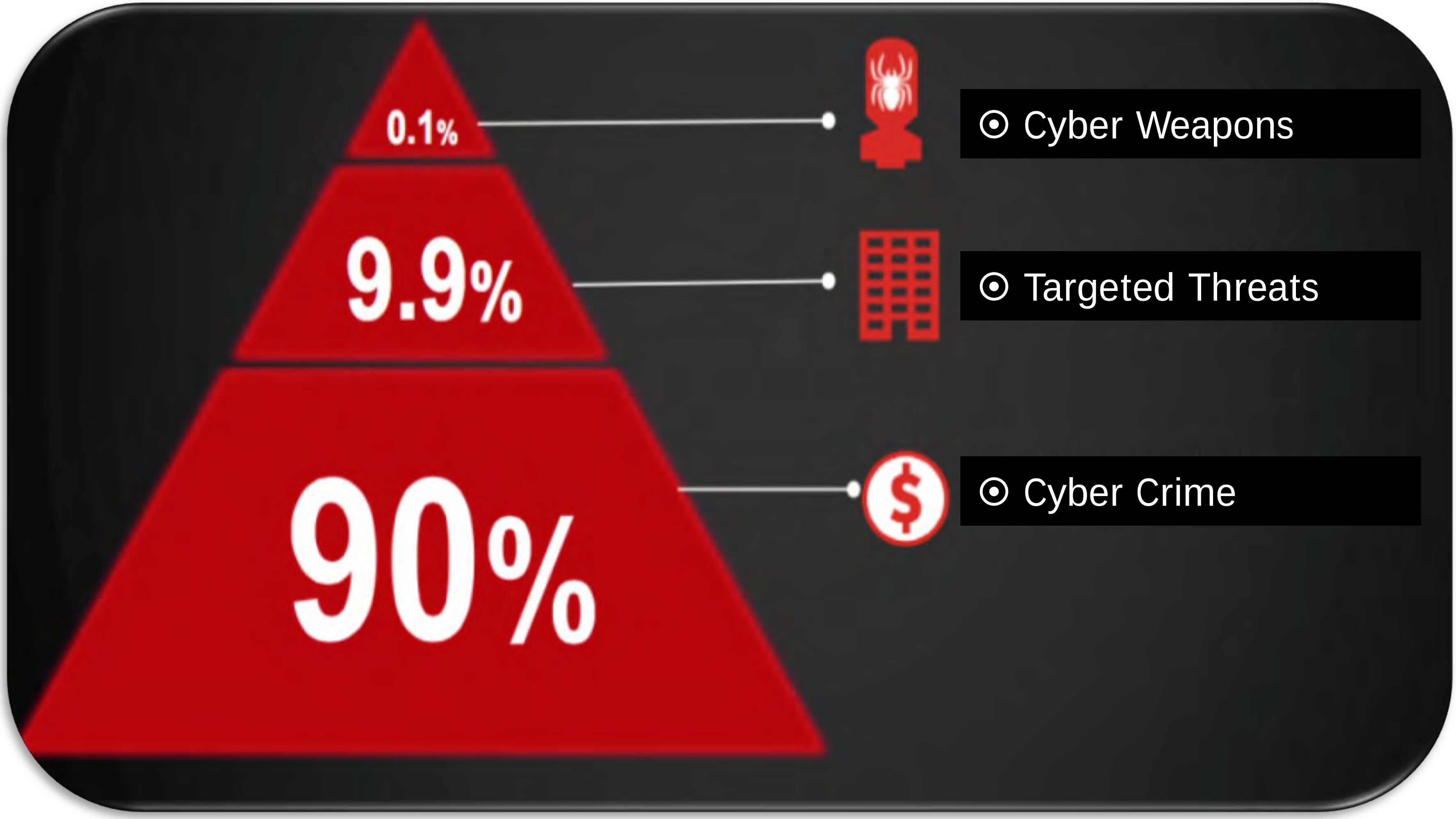


Type of Login	Prices
US bank with fullz info	2% of balance
EU bank with fullz	4–6% of balance
PayPal, Moneybookers, Netteier verified	6–20% of balance
Western Union transfer	10% from amount


EVERYTHING IS CONNECTED,
EVERYONE IS VULNERABLE
AND WHAT WE CAN DO ABOUT IT
FUTURE
CRIMES
MARC GOODMAN

WHAT´s NEXT??

⊙ Threats Pyramid



- ⊙ Cyber Weapons
- ⊙ Targeted Threats
- ⊙ Cyber Crime

$
MONEY

THANKS FOR YOUR ATTENTION

GRUPO DE DELITOS TELEMATICOS
UNIDAD CENTRAL OPERATIVA

gdt@notificaciones.guardiacivil.es

www.gdt.guardiacivil.es

Grupo de Delitos Telematicos

GrupoDelitosTelematicos

@GDTGuardiaCivil

GDT
GRUPO DE DELITOS TELEMÁTICOS