EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

botconf

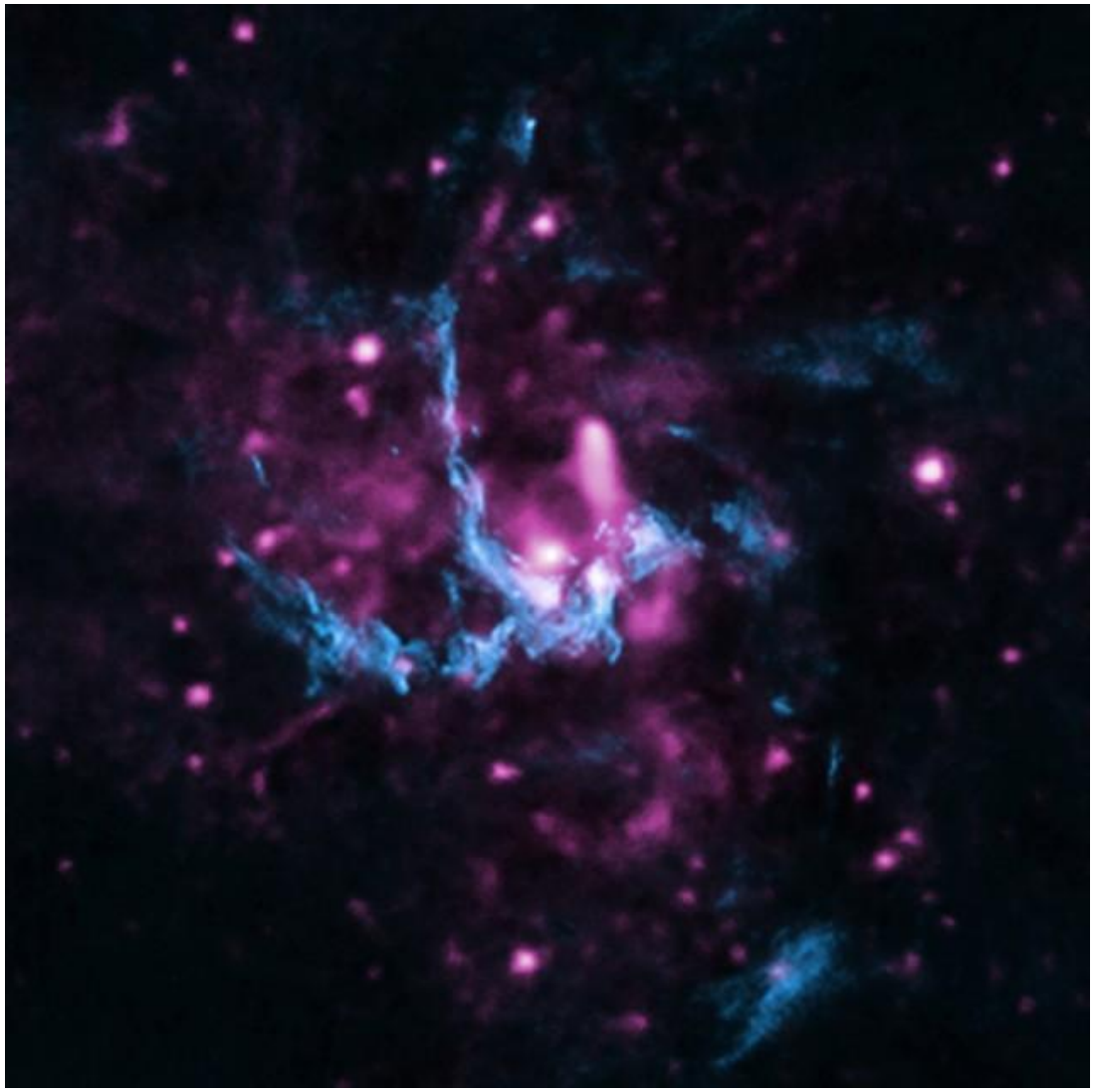
First botnet fighting conference 2013

EC3

Law Enforcement Action against Botnets

Jaap van Oss,
Team Leader Cybercrime
European Cybercrime Centre (EC3)
@jaapvoss

Trending topics?



What's new

Datum: 2005-06-03 08:18:00 **Verzender:** "dersox@gmail.com" **Onderwerp:**Re: irc **Time:** 09-08-2005 16:19:07pm**Bericht:**yeah, lets started once and get filthy rich :))

one important thing left though - just notice [redacted] is changing urls once in a while, so the correct tabs for it are:

{"[redacted]", "/fp/1_2",
"/lio-testdir2/http/[redacted]
/uk/bp/fp/1_2l/online/1,,logon,00.html", false},

cause first it was "fp/1_2l", then "fp/1_2m" and now its "fp/1_2n" -
so i think its better to left it "fp/1_2"
- so change this also pls, because its a pretty big bank in uk.

Outset of the EU 'botnet' scenery

- EU Cybersecurity Strategy
  - An Open, Safe and Secure Cyberspace

- Directive 2013/40/EU on Attacks against Information Systems
  - introduces the committing of crimes where "a significant number of information systems have been affected through the use of a tools" (i.e. botnet attacks)

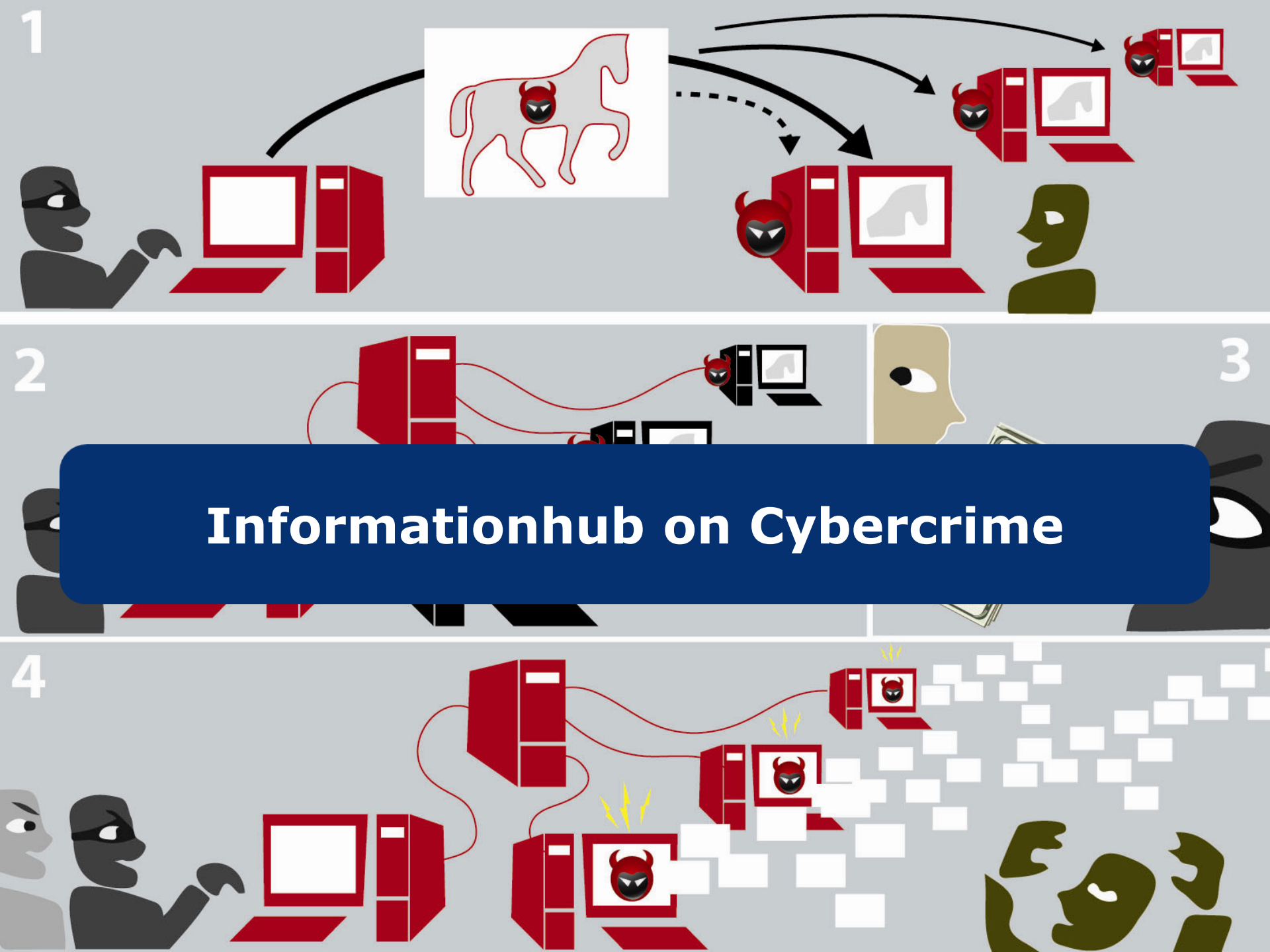
- Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre
  - facilitate cross-community information sharing on a range of issues, including early warning of cyber threats, and collaborative "task force" style responses

Cybercrimes committed by Organised Groups, particularly those generating large criminal profits such as online fraud;

Cyber attacks

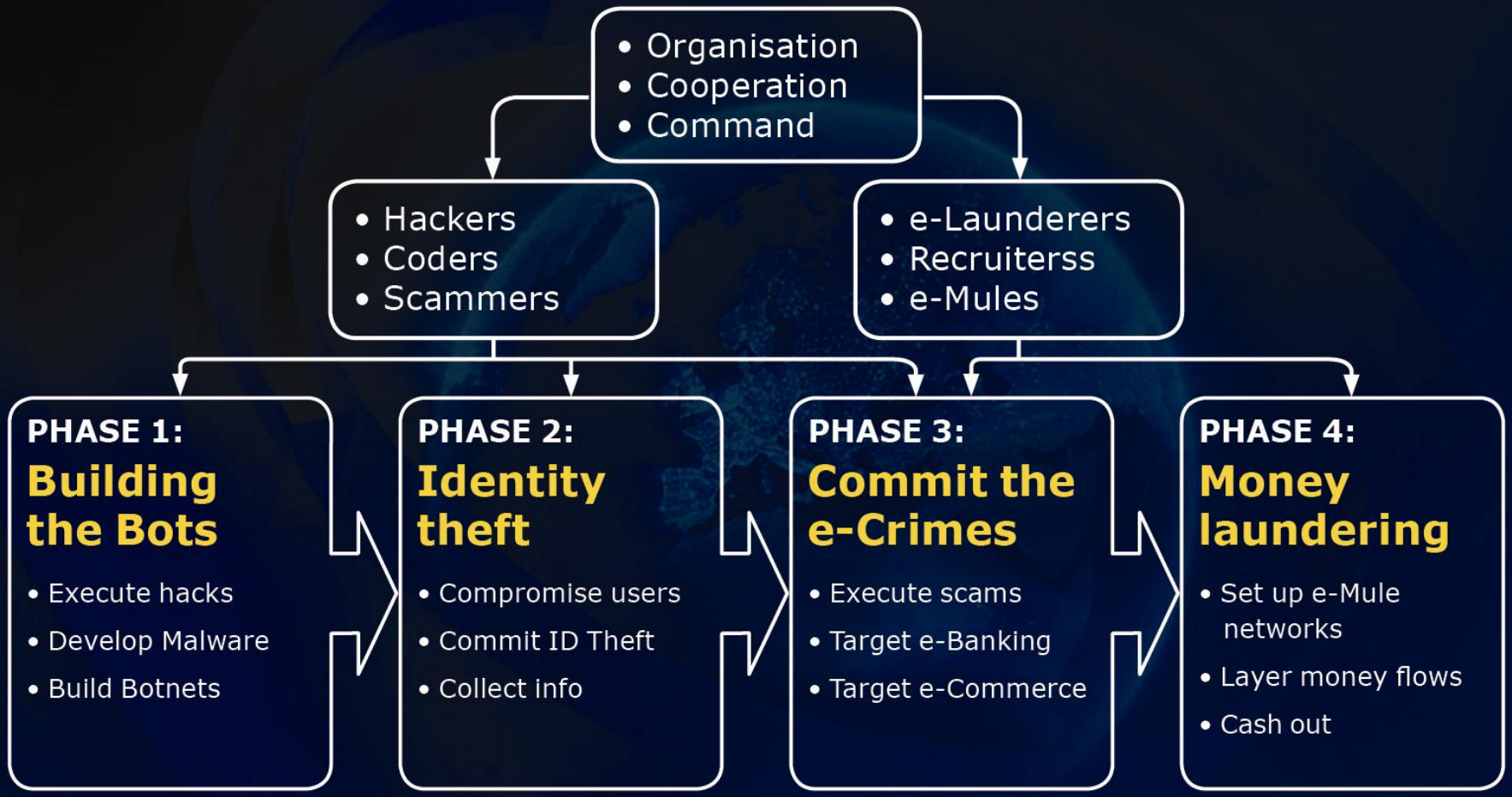
Images: Symantec, Confederation of European Security Services, Oilism.com

Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union.



Informationhub on Cybercrime

THE CYBERCRIME BUSINESS MODEL



Underground economy

Trade of stolen goods, stolen information, malware, tools, expertise and skills.

EUROPOL

FP Cyborg – Europol's instrument

FP CYBORG

- Building a cross-border information position on active groups
- Group structures, roles, Modus operandi, Routes for or money, Sequences of events; etc

Focus of CYBORG on Cybercrime

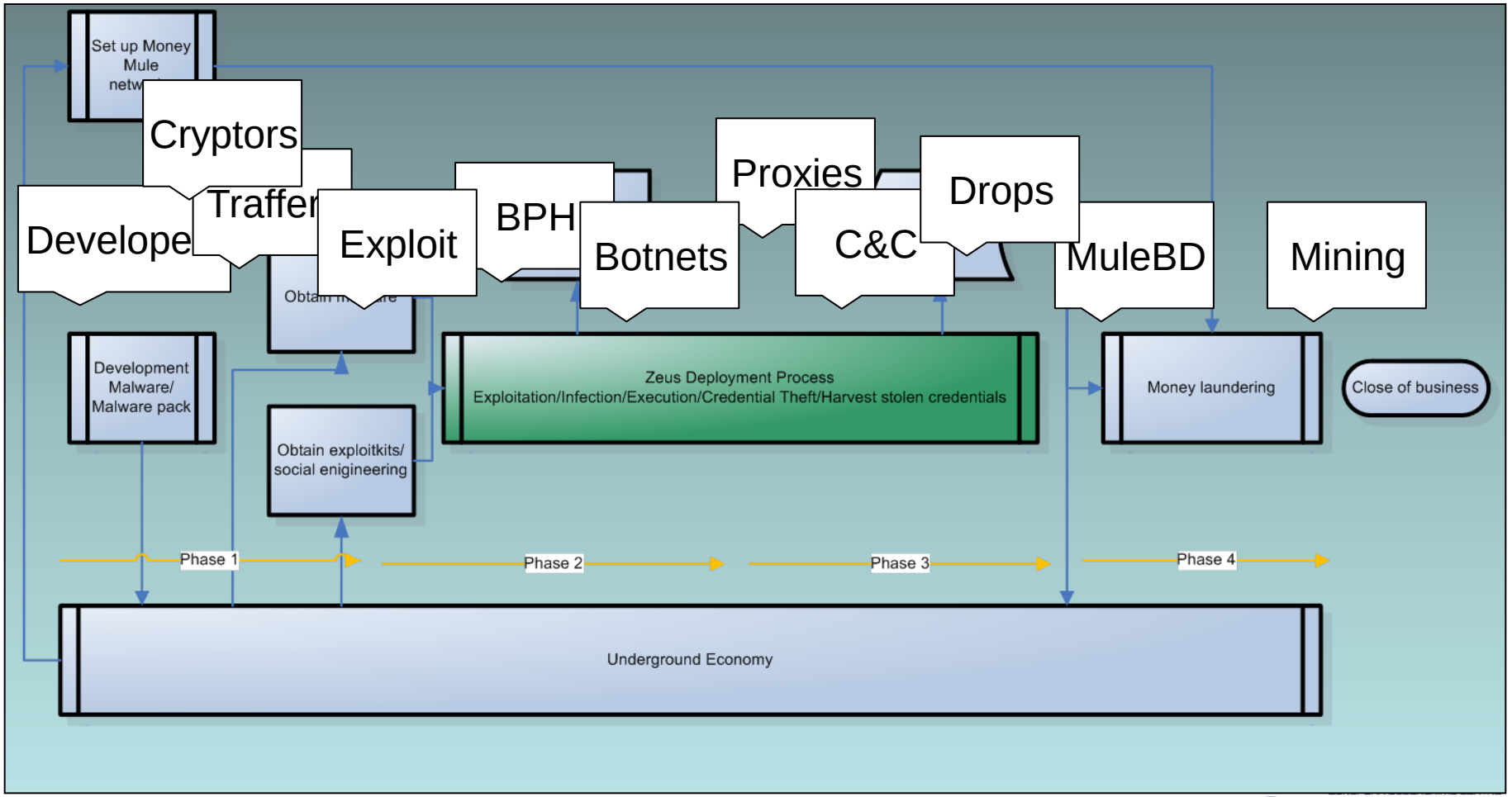
- Focus on Internet/ICT driven organized crime aiming at financial gain
- Crimes defined in the cyber crime convention (art. 2-8) including but not limited to ID theft, e-banking scams, and e-commerce fraud and e-laundring

Primary goal

- To support on-going investigations or to initiate new cross-border cases

EUROPOL

Deployment of Zeus Banking Trojan



Infrastructure is key?

victims of all kind

researchers
Intelligence
industry experts
(law enforcement)
AV industry
hackers
bloggers
malware-fighters
…

coders
traffers
exploiters
herders
crypters
BPH providers
cashers
receivers
...

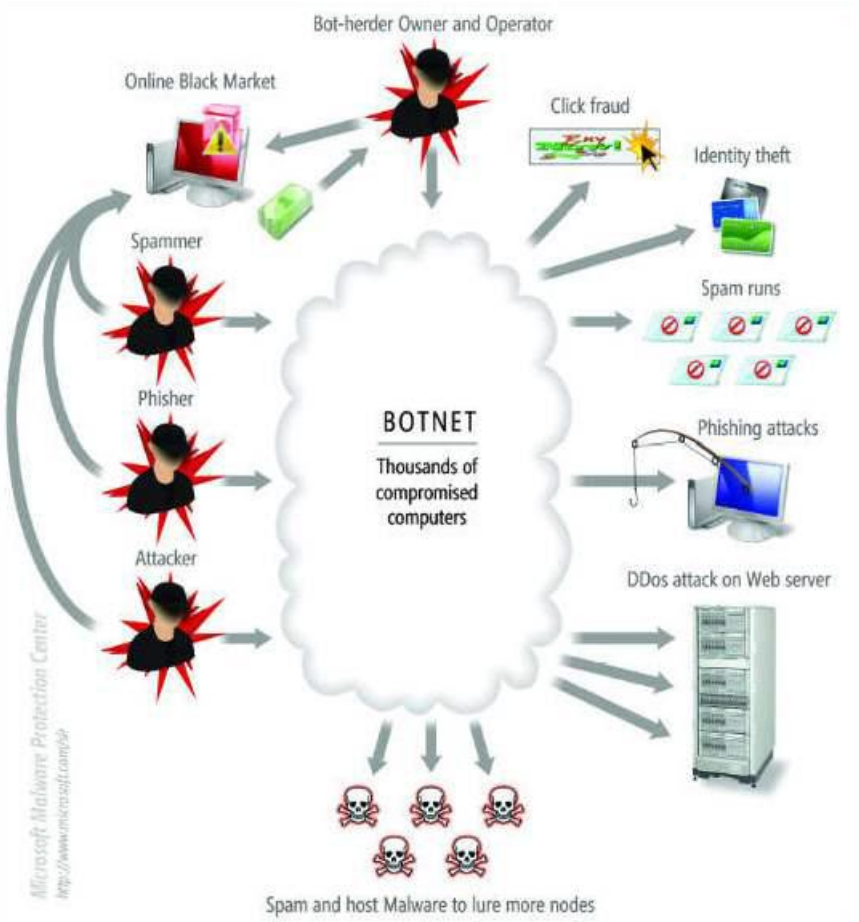
providers of all kind

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Challenges

Challenges:

- Multiple jurisdictions
- Cross-border coordination
- Information vs evidence
- Action vs investigation
- Legality
- Monitoring
- Protocols of information exchange



Law Enforcement action

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

ZeroAcces

ZeroAccess from Russia with love?

Posted on 29/11/13 - 13:59 in Threat Vectors » Malware

Here is a malicious email that carries the ZeroAccess botnet.

Mail Body	
	HiMy name is Anastasia.I am from Russia.Look my photo in attachment. <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"> <html> <head> <meta http-equiv="content-type" content="text/html; charset=UTF-8"> </head> <body bgcolor="#ffffff" text="#000000"> Hi My name is Anastasia. I am from Russia. Look my photo in attachment. </body> </html>
Attachments	
1	DSC_0178(copy).jpg.zip

cfg: https://www.virustotal.com/en/file/bb414f0dba516f686b2871228f491e72342b5ede539d0b6edfa5a1882a78f37e/analysis/

BIN: https://www.virustotal.com/en/file/c497e9f4319c6e81c63ea182a6e1833f8d74eefd17423a39cf3217a721958c35/analysis/

Tags: malware, botnet, russia, malicious email, ZeroAccess

Reference: https://twitter.com/malpush/status/406321624422436865/photo/1/large

Latest Threats

- 12:56 Syrian General Organization of Radio and TV DDoSed as par
- 12:59 Syrian Baath Media DDoSed as part of #OpSyria - 3 Decemb
- 13:02 Angolan Embassy in Israel DDoSed as part of #OpAngola - 2
- 12:53 "Buy $500 antivirus from us," says cybercriminal
- 13:01 Citadel/Zeus: rag.su

Trending

1. @Maxn3y
2. #OpGabon
3. @Anonymous
4. Israel
5. #OpSyria

Calendar - December 2013

M	T	W	T	F	S	S
25	26	27	28	29	30	1

MEDIA CORNER
Europol Media Corner
Press releases
News
Events
Corporate Publications
Early Warning Notifications
Strategic Analysis Reports
Public Documents
Crime Prevention Advice
Image Galleries
Video Gallery
Corporate identity
TV, Films and Books

Share:
Print friendly page | Print as PDF

NOTORIOUS BOTNET INFECTING 2 MILLION COMPUTERS DISRUPTED

5 December 2013

A rampant botnet has been successfully disrupted in a transatlantic operation involving Europol's European Cybercrime Centre (EC3) and law enforcement cybercrime units from Germany, Latvia, Luxembourg, Switzerland and the Netherlands as well as Europol's European Cybercrime Centre (EC3). Furthermore the operation was supported by Microsoft Corporation's Digital Crimes Unit and other technology industry partners.

The targeted botnet, known as Zeroaccess, is responsible for infecting over 2 million computers worldwide, specifically targeting search results on Google, Bing and Yahoo search engines, and is estimated to cost online advertisers US$ 2.7 million each month. Today's action is expected to have significantly disrupted the botnet's operation, increasing the cost and risk for the cybercriminals to continue doing business and freeing victims' computers from the malware. The botnet worked as a Trojan horse affecting Windows operating systems so that malware could be downloaded.

Microsoft filed a civil suit against the cybercriminals operating the Zeroaccess botnet, and received authorisation to simultaneously block incoming and outgoing communications between computers located in the U.S. and the 18 identified Internet Protocol (IP) addresses being used to commit the fraudulent schemes. Due to Germany's initiative Europol's European Cybercrime Centre (EC3) coordinated a multi-jurisdictional criminal action targeting 18 IP addresses located in Europe. Thanks to the efforts of EC3 and the involved agencies search warrants and seizures on computer servers associated with the fraudulent IP addresses were executed in several of the involved countries.

Thank you

@jaapvoss