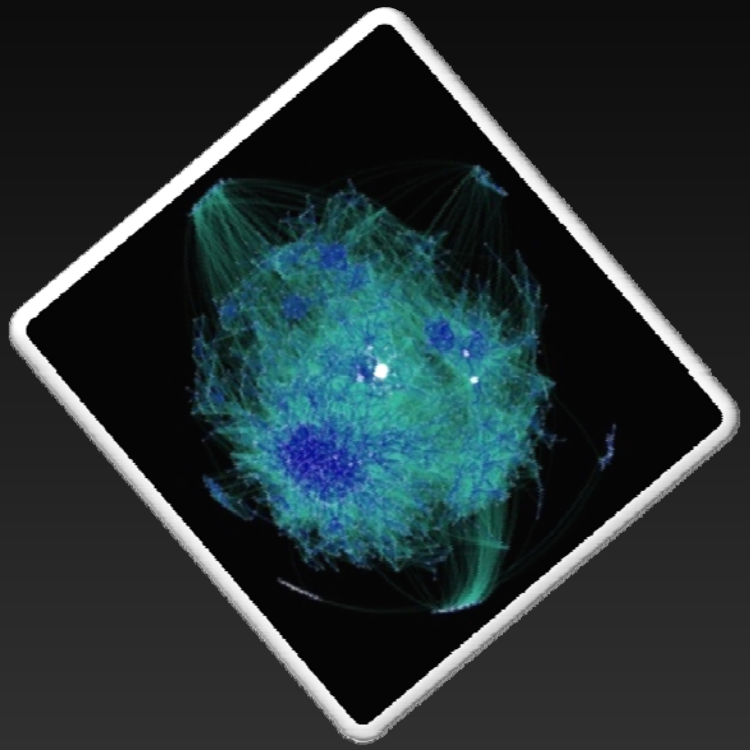
Fighting against Botnet

MaX

(maxoverpro@gmail.com)

Agenda

- Introduction to Botnet.
- Botnet History.
- Recent Botnet Trends.
- Botnet Life Cycle.
- Botnet Communication.
- Use of Botnets.
- Botnet Economics.
- Botnet Analysis.
- Botnet detection and response.
- Demonstration.



Introduction to Botnet

Bot(Zombie, Robot) :

In an automated way to perform functions for the program.

Bot Client :

Infected machine.

Botnet :

Bots connected to a particular channel.
(IRC, HTTP, P2P, WEB, I.M)

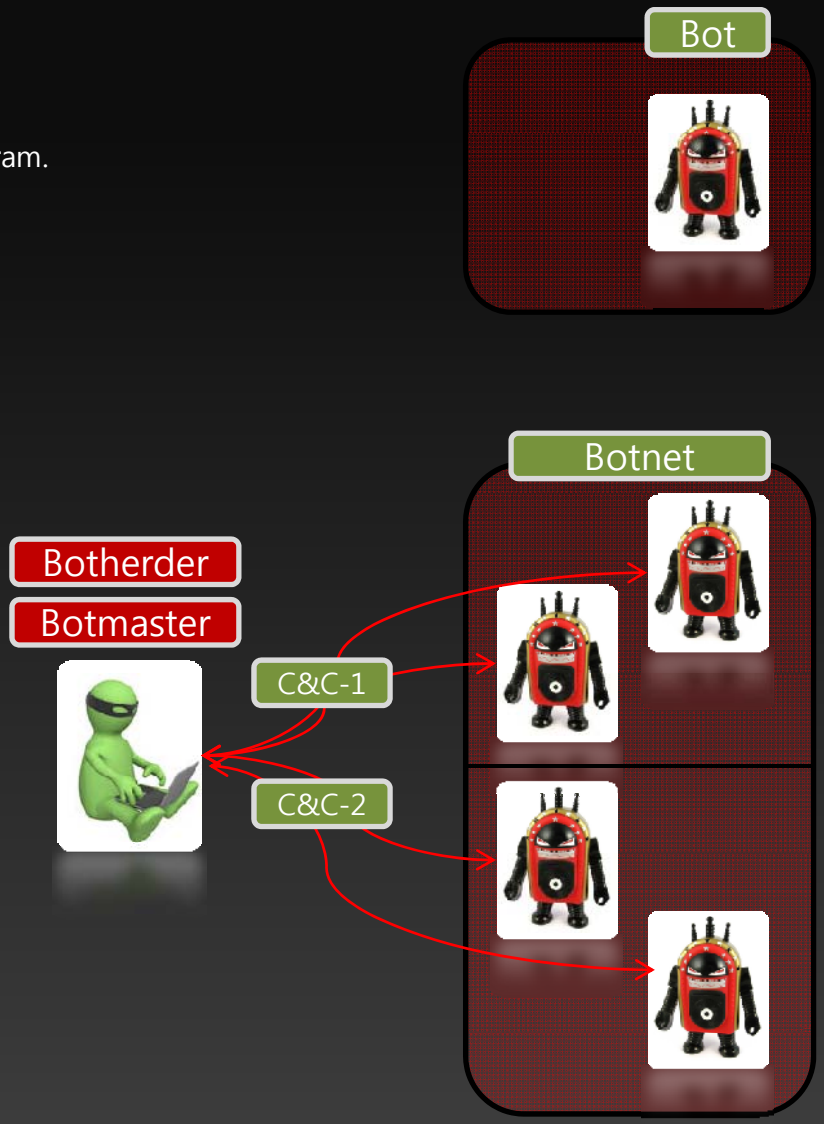
- Controlled by Botmaster or Botherder.

Botmaster or Botherder :

Can control the group remotely.

C&C(Command and Control) :

- Communication channel for Command and Control.



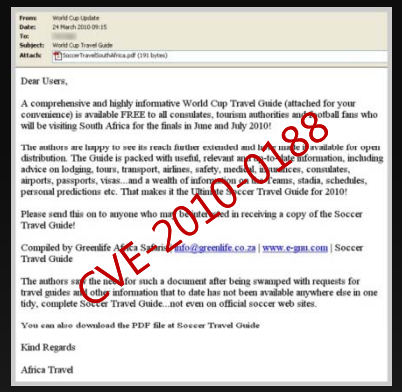
Introduction to Botnet

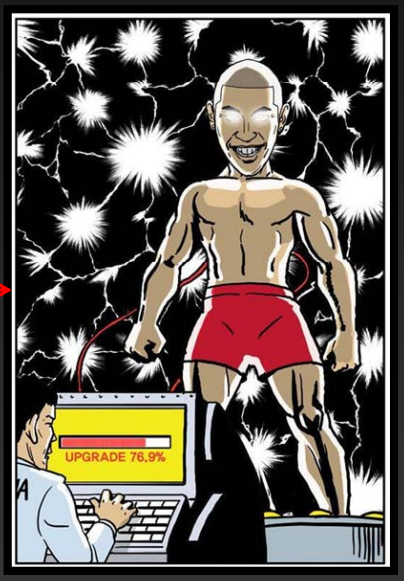
Like it!

Botmaster

Botnet
Join

Bot

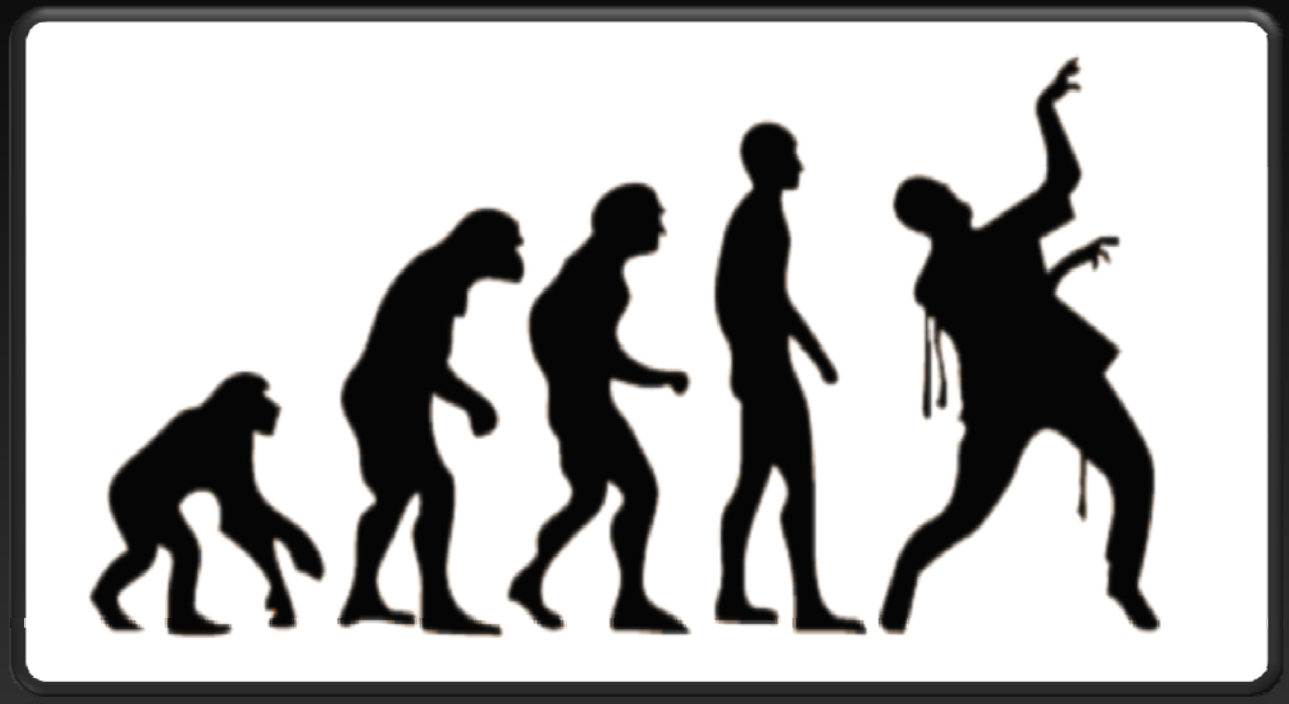




Bot Update

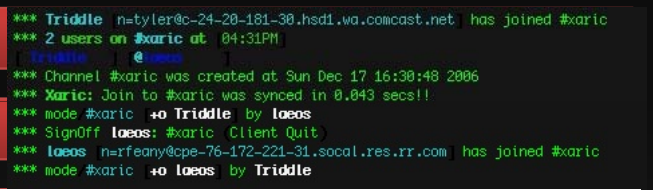
0-Day

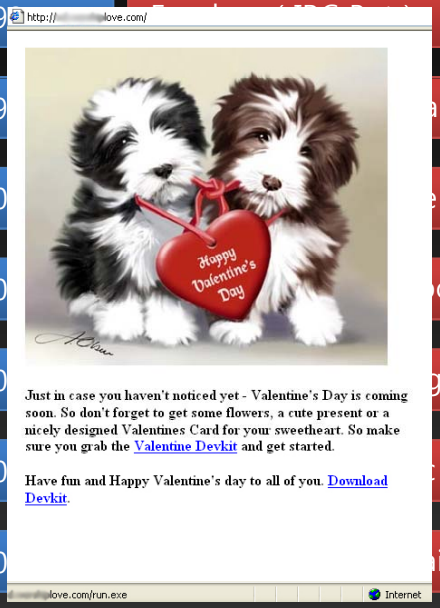
Botnet History

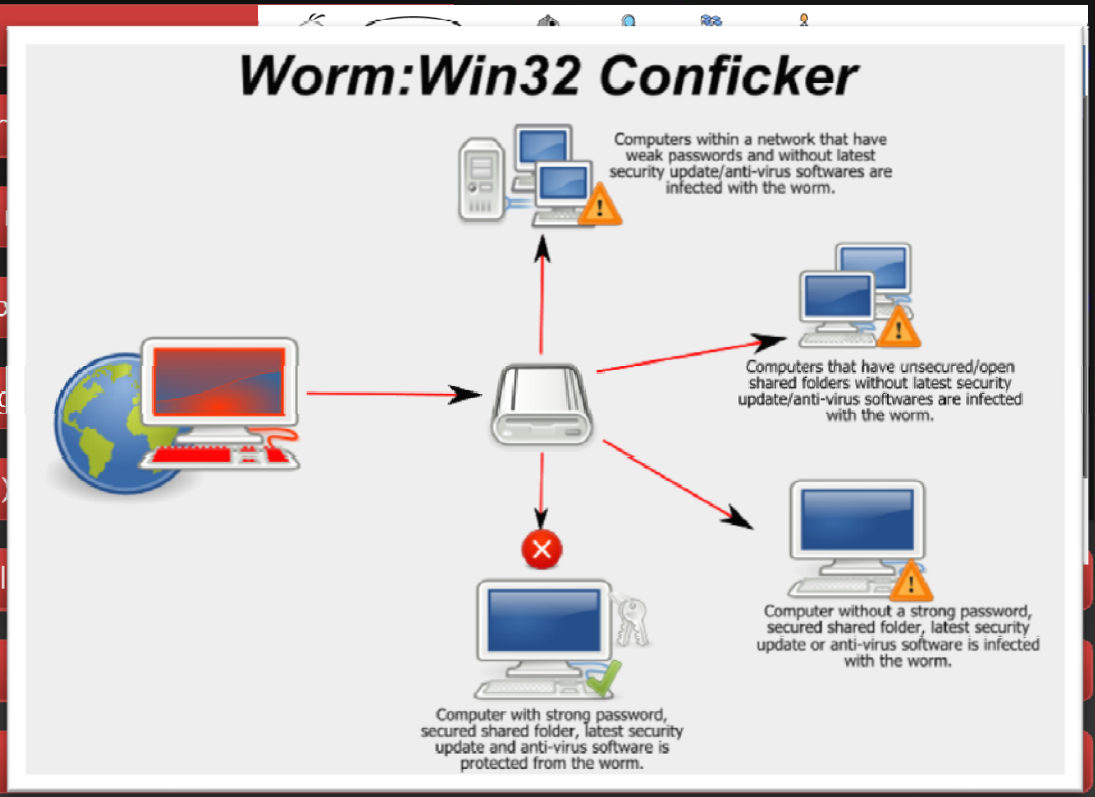


Botnet History

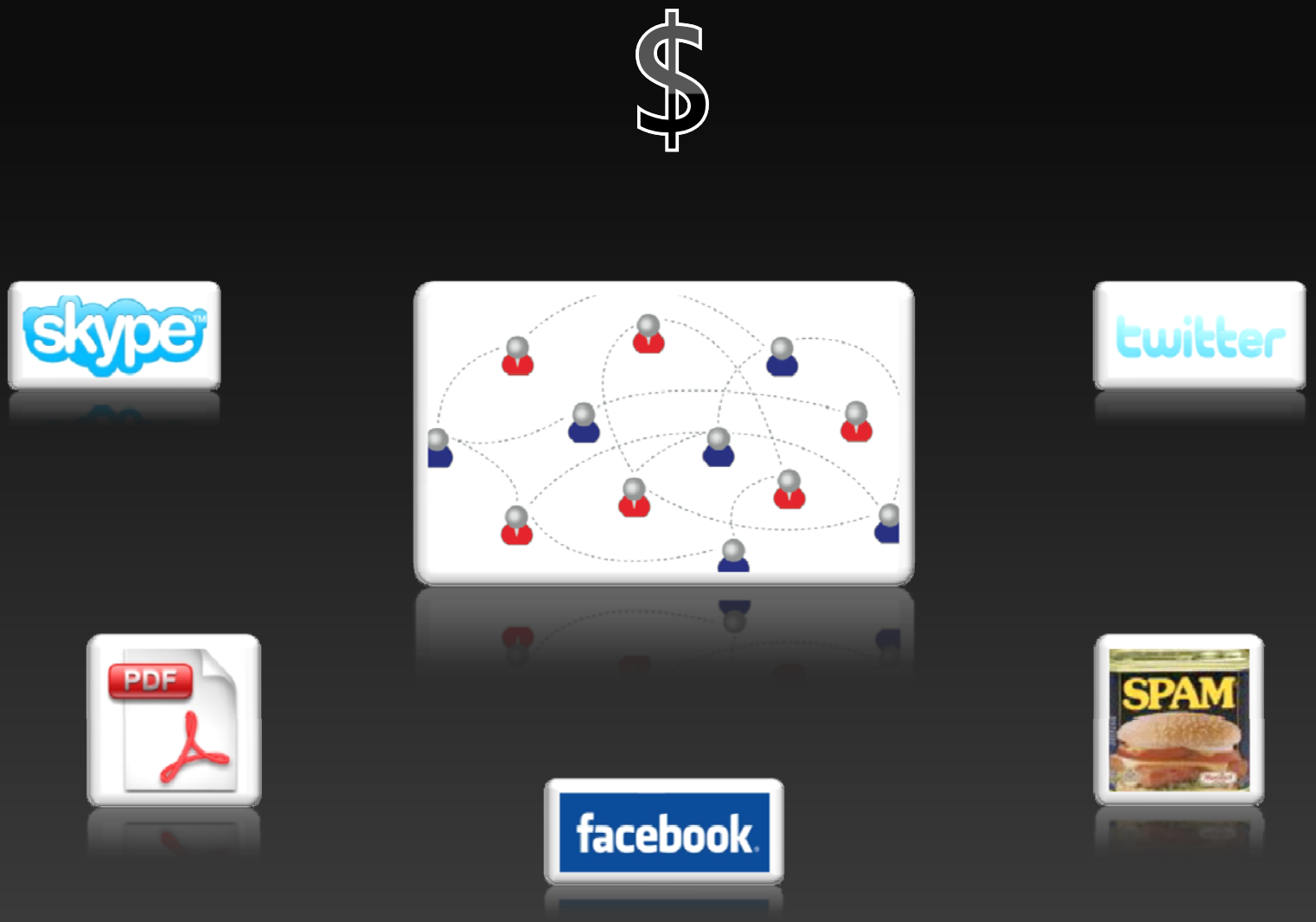
1988	Invention of IRC
1989	Greg Lindahl (GMBot/Hunt the Wumpus - IRCBot)
199	
199	
200	
200	
200	
200	
200	
2007	StormWorm
2008	Waledac, Conficker
2009	Mariposa







Recent Botnet Trends



Botnet Life Cycle

Exploitation

- Malicious Code.
- Unpatched Vulnerabilities.
- Backdoor.
- Worm.
- Remote Access Trojans.
- Password Guessing.

Rallying / Secure Botnet

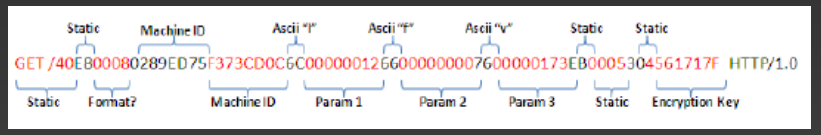
- Join Botnet
- Kill Anti-Virus
- Hidden
- Downloader
- Rootkit

Listen / Payload

- Botnet command.
- Payload
- Update

Command : Erase

- Erase Evidence.
- Bot



Botnet Communication (Infection Channel)

- E-Mail
- Instant Messenger
- Social Network
- Downloader (Malicious Site)
- P2P
- File shareing

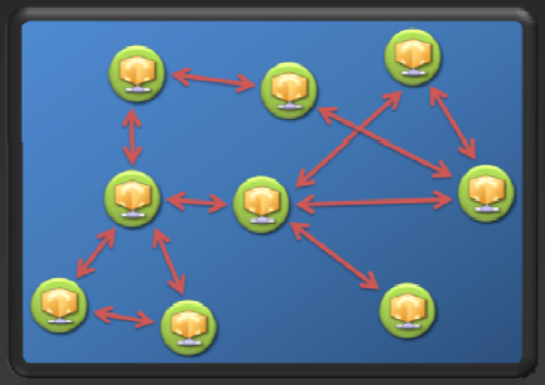
Botnet Communication (Topology)

Star

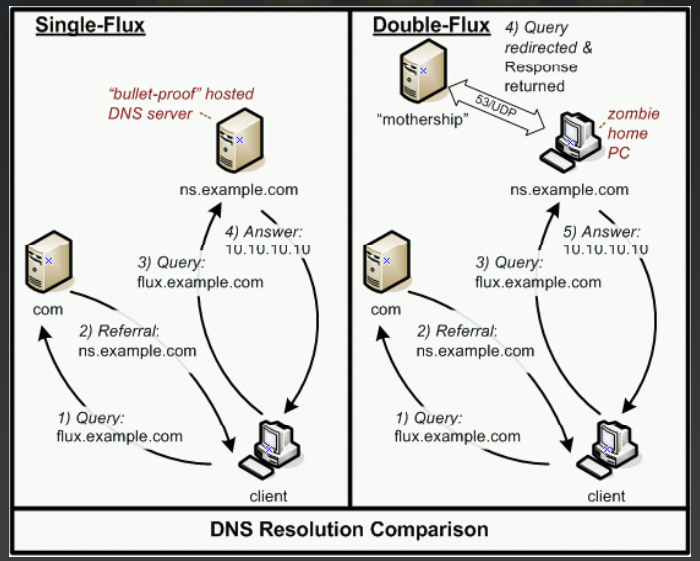
Multi-Server

Hierarchical

Random

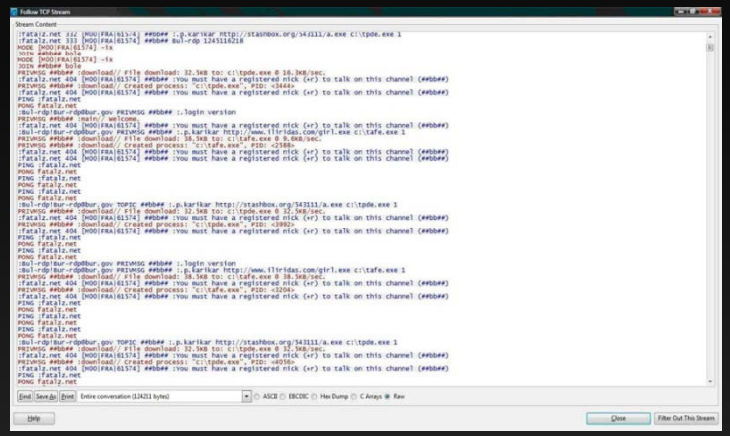


Fast-flux

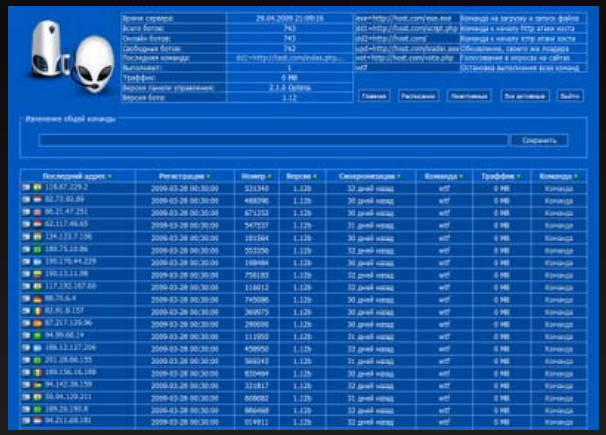


Botnet Communication (Protocols)

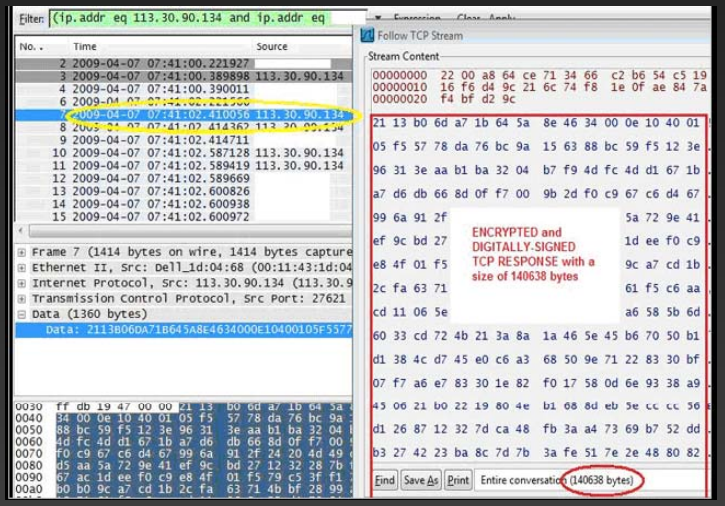
IRC



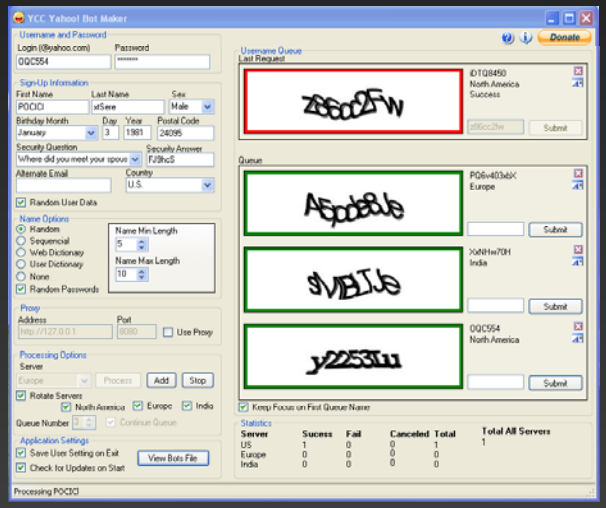
HTTP



P2P



I.M

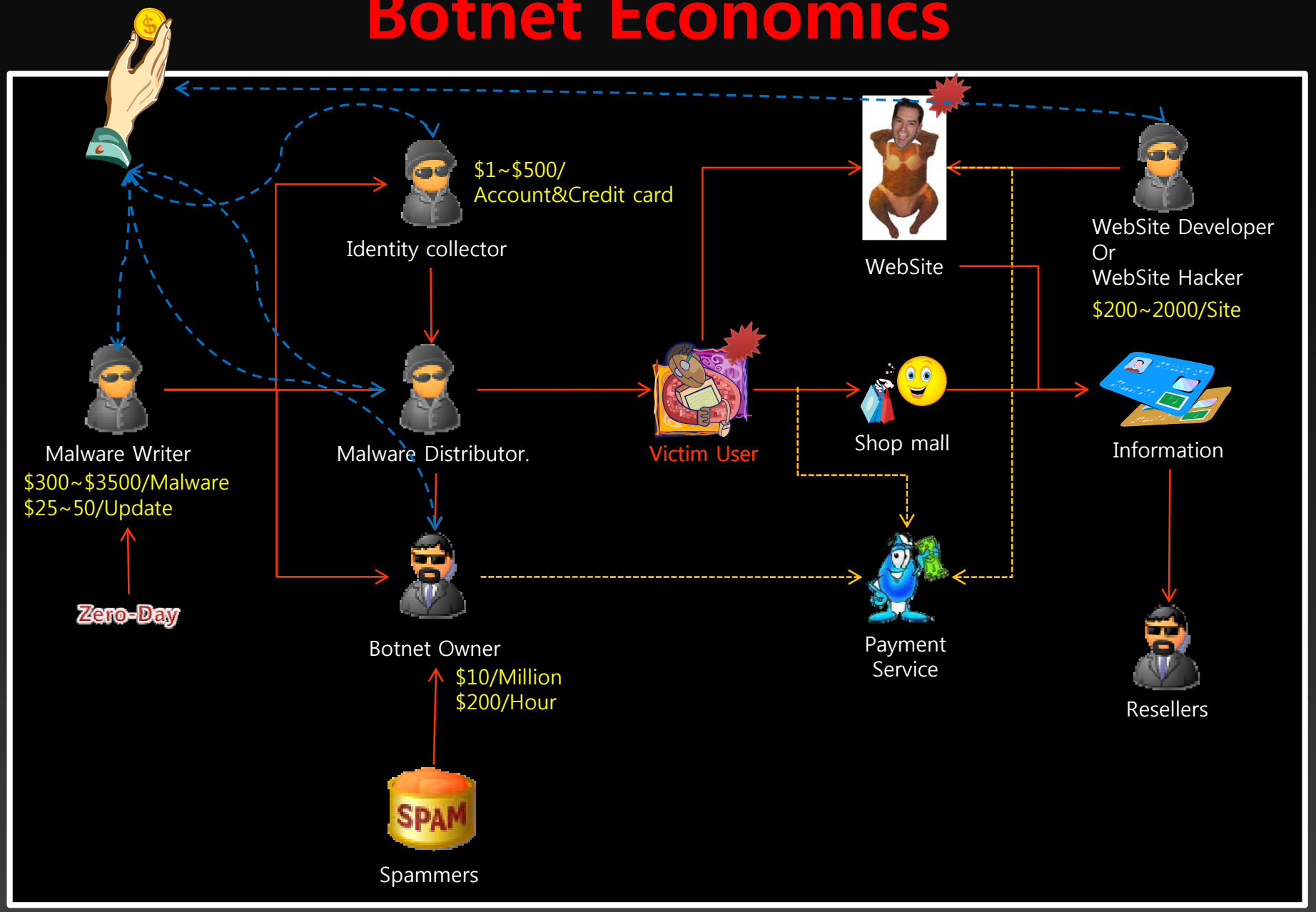


...

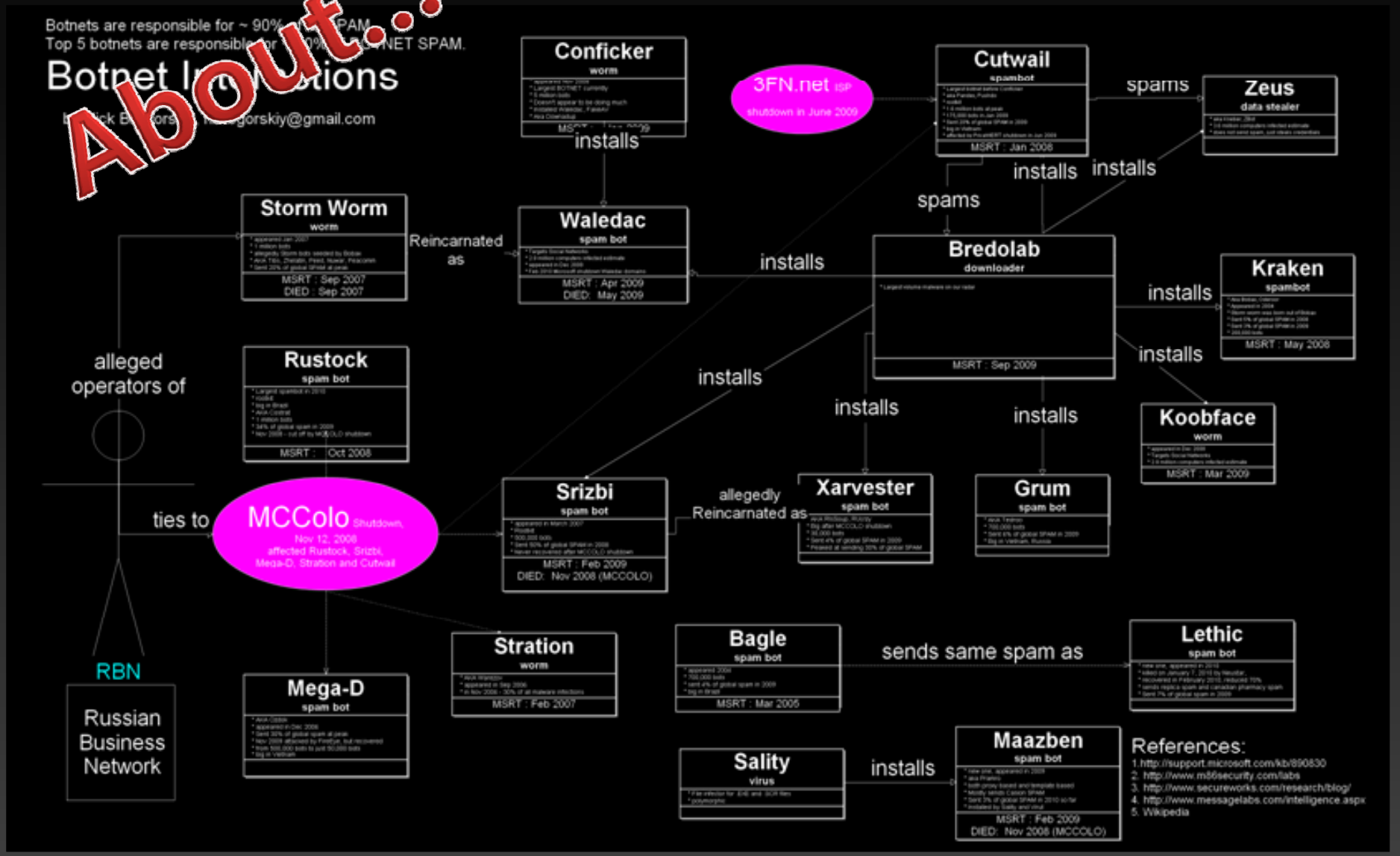
Use of Botnet

- Phishing
- Spam
- DDoS
- Click Fraud
- Adware/Spyware Install
- Information theft
- Keystroke Logging
- Stealing information or files

Botnet Economics



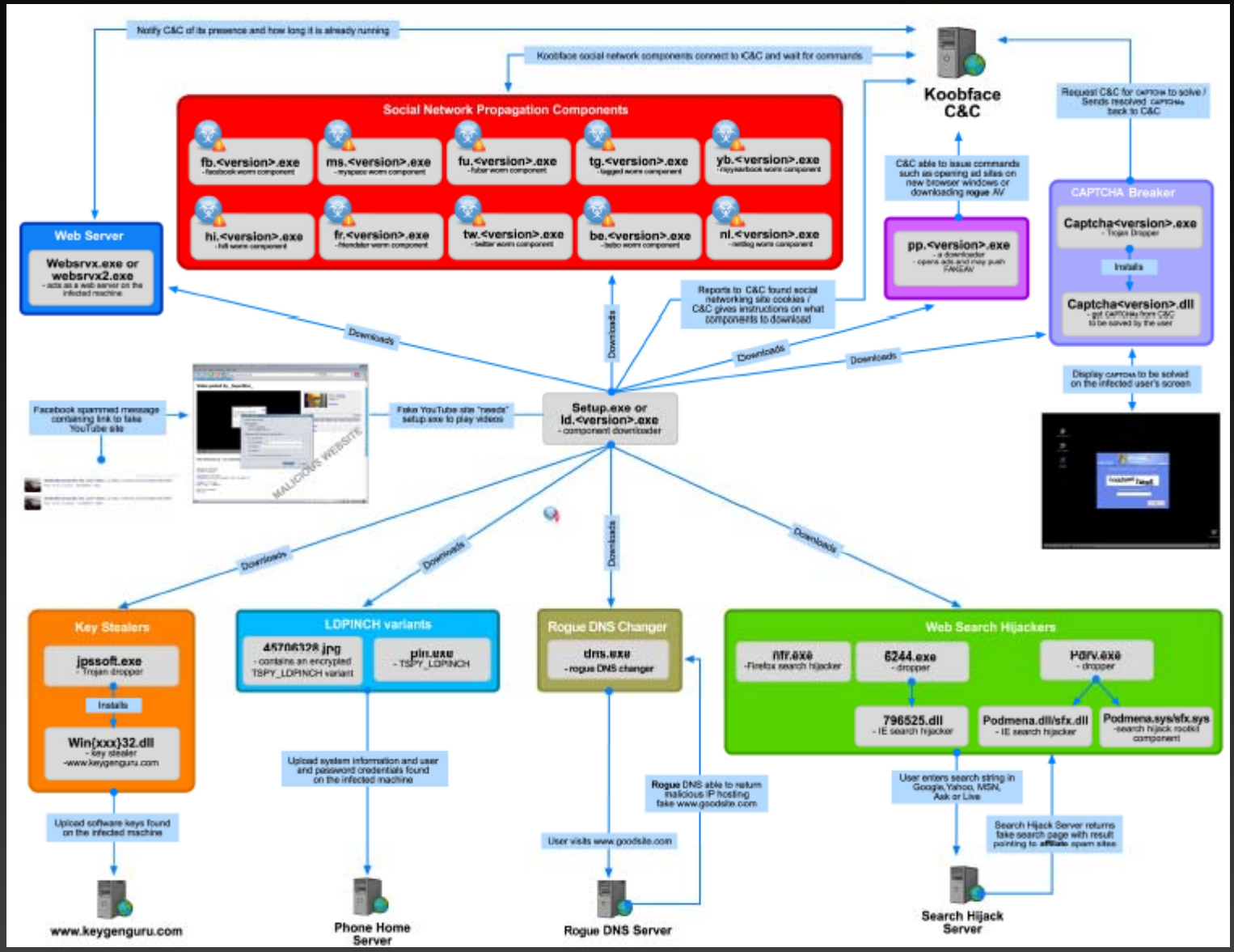
Botnet Analysis



Botnet Analysis

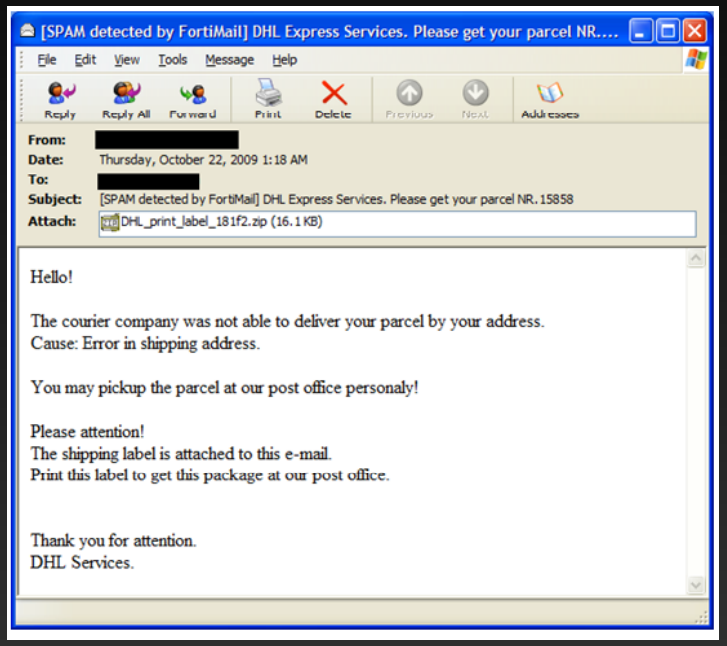
SpamBot	Worm	Downloader	Data Stealer
• Mega-D • Rustock • Waledac • Srizbi • Cutwail • Kraken • Grum • Xarvester • Bagle • Maazben • Lethic	• Storm Worm • Conficker • Stration • **Koobface**	• **Bredolab**	• **Zeus**

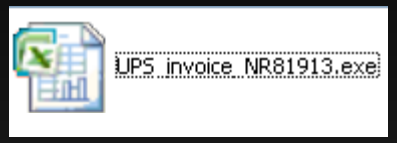
Botnet Analysis / Koobface

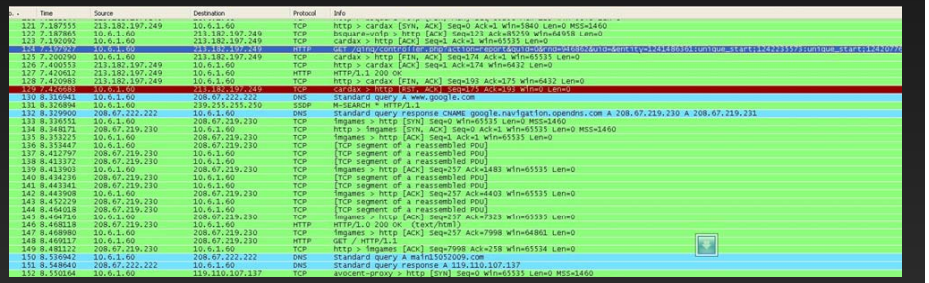


Botnet Analysis / Bredolab

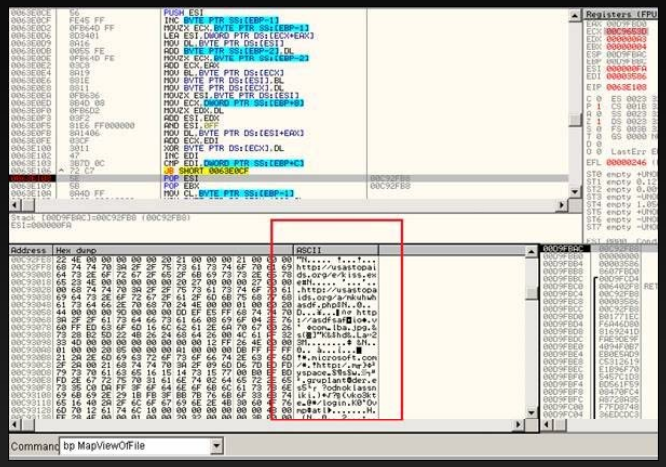
1St Bredolab : MS07-017 (GDI Local Elevation of Privilege Vulnerability) / CVE-2006-5758
2nd Bredolab : MS08-025 (Windows Kernel Usermode Callback Local Privilege Escalation Vulnerability) / CVE-2008-1084
3rd Bredolab : Flow Allows local users with the SeDebugPrivilegge privilege to execute arbitary code as kernel / CVE-2004-2339



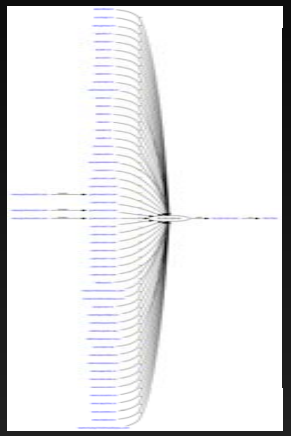




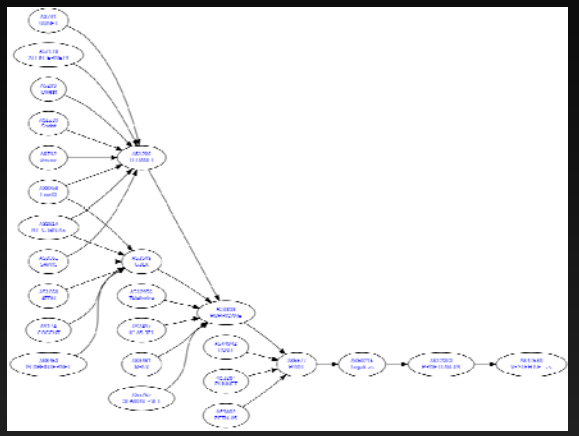
Botnet Analysis / Zeus

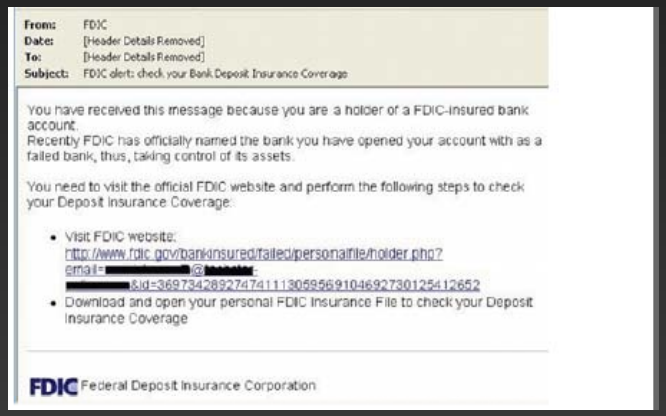


Zeus C&C



NameServer





From: FDIC
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: FDIC alert: check your Bank Deposit Insurance Coverage

You have received this message because you are a holder of a FDIC-insured bank account.
Recently FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets.

You need to visit the official FDIC website and perform the following steps to check your Deposit Insurance Coverage:

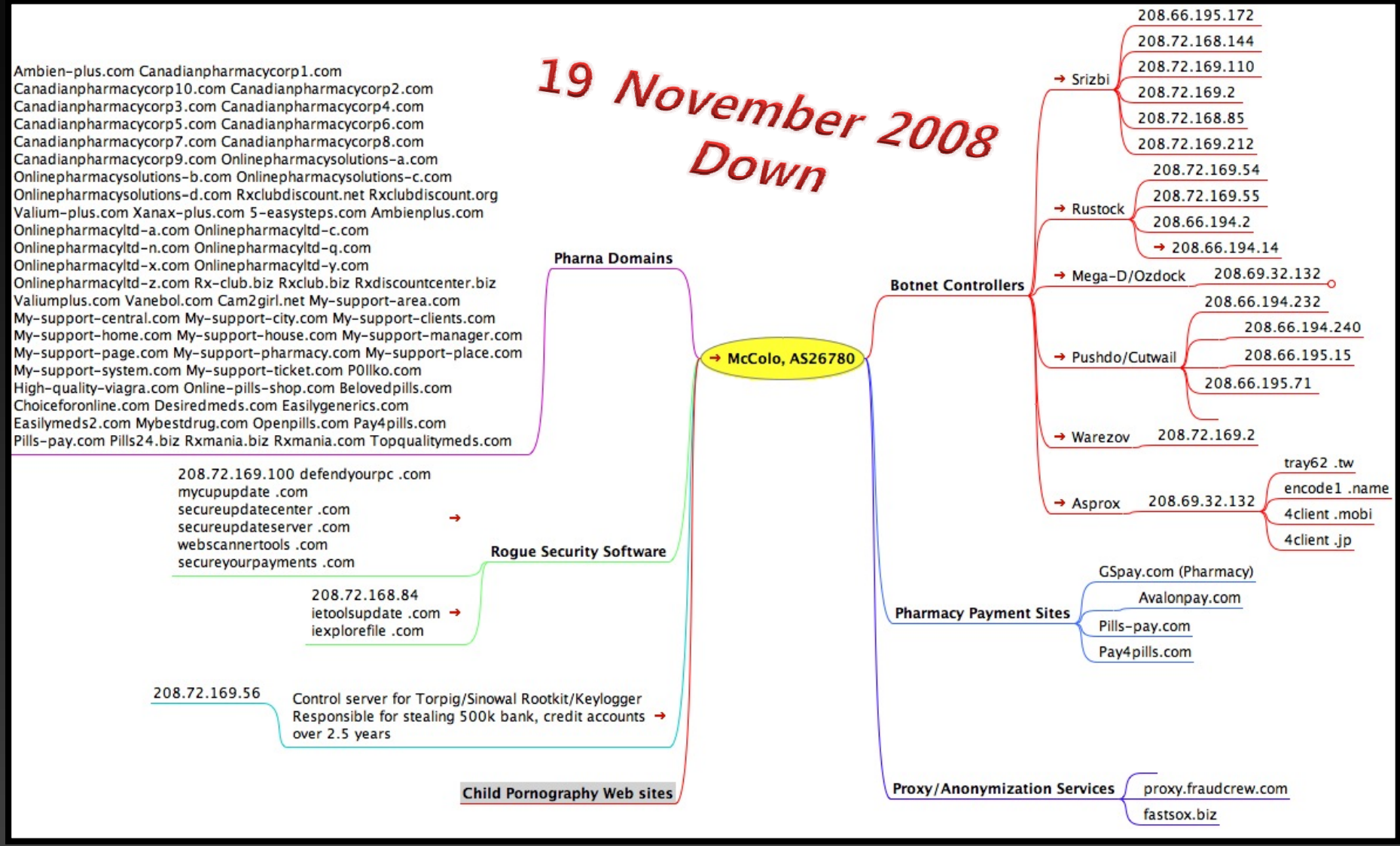
- Visit FDIC website:
  http://www.fdic.gov/bankinsured/failed/personalfile/holder.php?
  email=[redacted]
  [redacted]&id=3697342892747411130595691046927301254126 52
- Download and open your personal FDIC Insurance File to check your Deposit Insurance Coverage

FDIC Federal Deposit Insurance Corporation

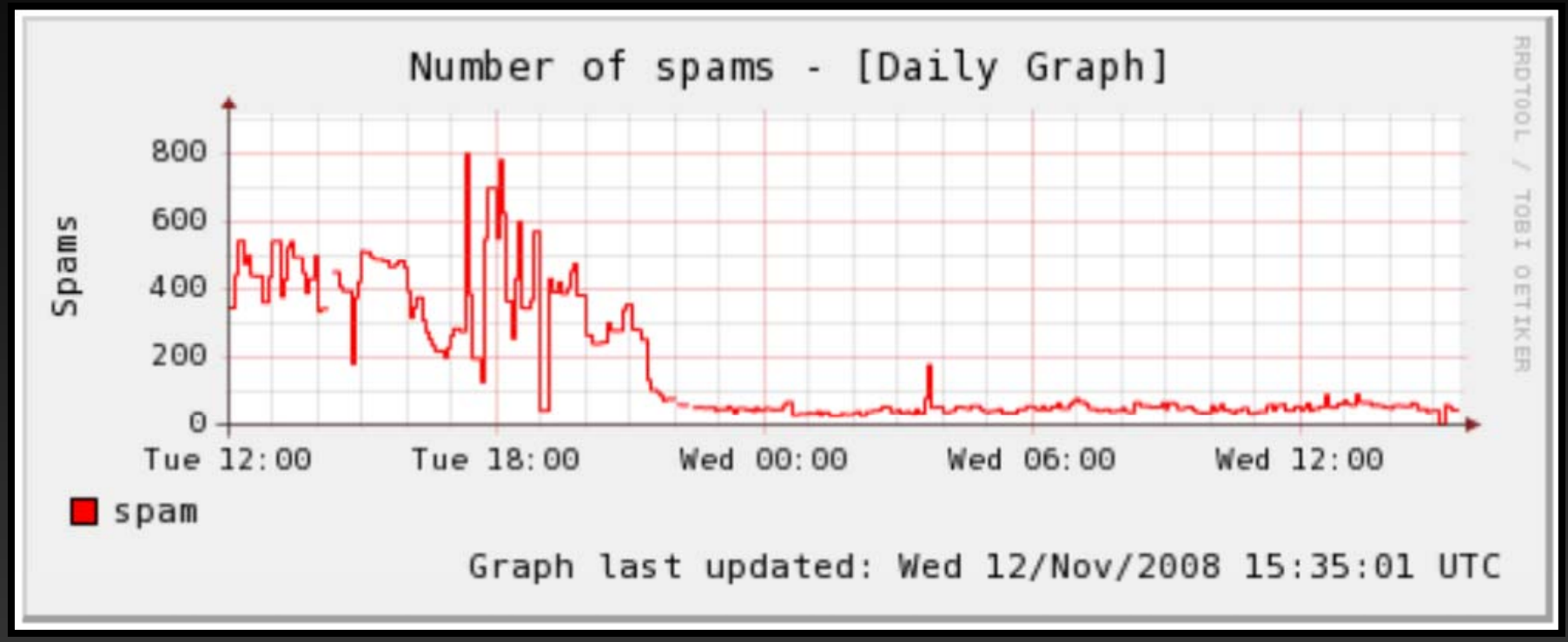
Botnet detection and response

- Anti-Virus
- IDS
- IPS
- F/W
- C&C Down.
- ~-....

Botnet Analysis



Botnet Analysis



Demonstration

Caution!

해킹자료.공격기 | [redacted] 2010/06/12 19:10

http://blog.naver.com/[redacted] 복사

해킹자료 팝니다 !

아이피와 **홈페이지 공격기** 팝니다 !

해킹자료 : **넷봇6.0(VIP버전), 공격기(홈페이지포함) 등등**

공격 신청도 받습니다 !

10분안에 신청받은 컴퓨터 작살!!!

***공유기 불가 !**

[redacted] **으로 연락주세요 !**

아이피 : **1개당 5000원**

해킹자료 : **희귀성의 따른 가치성 그 자리에서 즉시 가격 선받음...!**

기타 해킹하는 법 : 1개당 2000원

IT.컴퓨터

덧글 쓰기 | 엮인글 쓰기 | 공감하기 이 포스트를..

PC방 관리 프로그램 원격 해킹툴 배포 일당 검거

기사등록일 2010.06.25 장윤정기자 linda@etnews.co.kr ▶ 기자의 다른 기사 보기

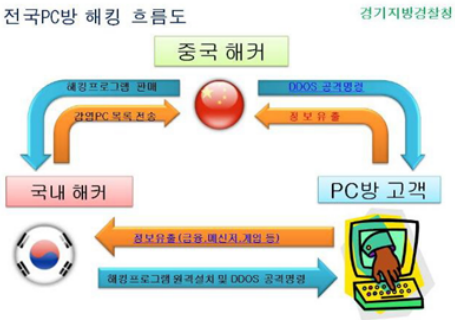
기사구매하기 | PDF보기 | 번역의뢰 한마디쓰기(0) -작게 | 기본 | +크게

[AD]최신 IDC보고서 받고 영화도 보고!

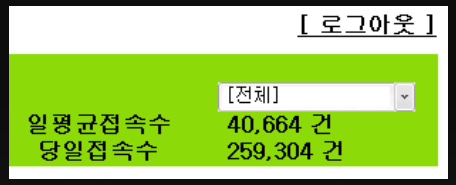
PC방 관리 프로그램으로 원격 해킹툴을 배포해 전국 700여 PC방에 약 1만1000대의 PC를 좀비 PC로 만들어 부당 이득을 챙긴 일당 33명이 검거됐다.

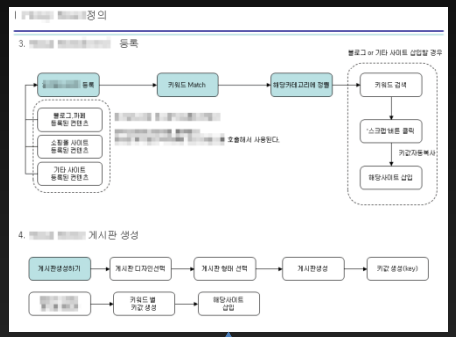
이 사건은 그간 보안에 취약한 PC방 실태로 인해 이미 예견된 범죄였다는 점에서 경종을 울리고 있다.

경기지방경찰청 사이버범죄수사대는 중국에서 구입한 '넷봇 어택' 해킹프로그램을 전국 PC방에 유포해 인터넷 게임

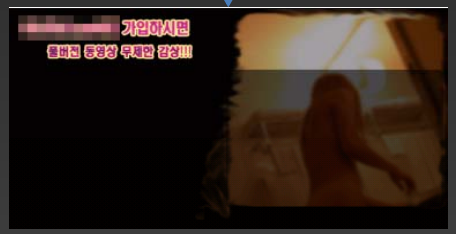


Caution!





AD? Bot?



가짜백신 유포해 36억 편취한 일당 13명 검거

[입력날짜: 2010-03-23 18:32]

스크랩 프린트하기 목록

49만여 피해자들 휴대폰 소액결제 피해 사실조차 몰라

인터넷 포털사이트 검색경로도 엿장수 마음대로 다양한 사이버범죄를 펼치며, 49만여 피해자들로부터 32억여원을 편취한 일당이 경찰에 검거됐다. 특히 지난 7.7DDoS대란 이후, 인터넷 보안의식이 높아지고 바이러스 치료의 중요성이 부각되면서 이를 교묘히 이용했다는 점에서도 주목된다.

경남지방경찰청(청장 조만기) 사이버수사대는 지난 3월 16일, 인터넷 이용자를 속여 몰래 설치되는 악성프로그램을 개발해 780여대의 컴퓨터에 유포·설치한 후 이를 이용해 광고수수료를 받아 챙긴 장모씨(34세) 및 악성코드 치료기능이 없는 가짜백신으로 휴대폰 소액결제를 유도하는 수법으로 피해자 18만 여명으로부터 15억5천여만원을 편취한 목모씨(29세) 등 악성프로그램 유포 및 가짜백신 운영자 등 피의자 13명을 검거해 이중 2명을 구속 송치했다고 23일 밝혔다.

Reference

[1] Botnet Communication Topologies, *Understanding the intricacies of botnet Command-and-Control* , Gunter Ollmann, VP of Research, Damballa, Inc.
[2] Spam declines after hosting company shut-down, by Robert Vamosi
[3] Botnets, the killer web app, Craig A.Schiller, Jim Binkley, Dvidd Harley, Gadi Evron, Tony Bradley, Carsten Willems, Michael Cross
[4] The economics of botnets, Yuri Namestnikov
[5] Botnet Communications and Detection, HKCERT
[6] Cyber Attack Trend and Botnet, S.C.Leung
[7] FastFlux&Zeus, Roman hussy
[8] Botnet Mitigation Methods, Kris Seeburn
[9] Botnets Attacks Trends, S.S.Sarma, CERT-In
[10] Botnet and Mass DDoS Attack, Heejo Lee, Hyunsang Choi, Korea University
[11] A Taxonomy of Botnet Structures, David Dagon, Guofei Gu, Christopher P. Lee, Wenke Lee, Georgia Institute of Techonology
[12] Bashing Botnets, Conficker Kills and other Service Improvements, Tom Le
[13] Botnet Detection and Response Technology, Mi Joo Kim
[14] Modeling Botnet Propagation Using Time Zones, David Dagon, Ciff Zou, Wenke Lee, Georgia Institute of Techonology
[15] Botnet Detection and Response, The Network is the infection, David Dagon, Georgia Institute of Techonology
[16] Web 2.0 Botnet Evolution KOOBFACE Revisited, Jonell Baltazar, TrendMicro
[17] The Business of Cybercrime / A complex Business Model, TrendMicro
[18] The Real Face of KOOBFACE : The Largest Web 2.0 Botnet Explained, Jonell Baltazar, Joey Costoya, RyanFlores, TrendMicro
[19] Cutwail Botnet, Alice Decker, David Sancho, Louciif Kharouni, Max Goncharov, Robert McArdle, TrendMicro
[20] Infiltrating WALEDAC Botnet's Covert Operations, Jonell Baltazar, Joey Costoya, RyanFlores, TrendMicro
[21] BREDOLAB's Sudden Rise in Prominence, David Sancho, TrendMicro
[22] Walowdac – Analysis of a Peer-to-Peer Botnet, Ben Stock, Jan Gobel, Markus Engelberth, Felix C. Freiling, Thorsten Holz

Q&A?

Thank you!