Cert-Lexsi

Dead angle (Torpig vs PRG)

CERT-LEXSI

LEXSI

Agenda

- Cert-Lexsi Presentation
- Torpig vs PRG: Introduction
- Ecosystems
- Propagation
- Clients code
- Infrastructure
- Targets
- Comparison and efficiency
- News

Cert-Lexsi Presentation

Cert-Lexsi is a French CSIRT Team:

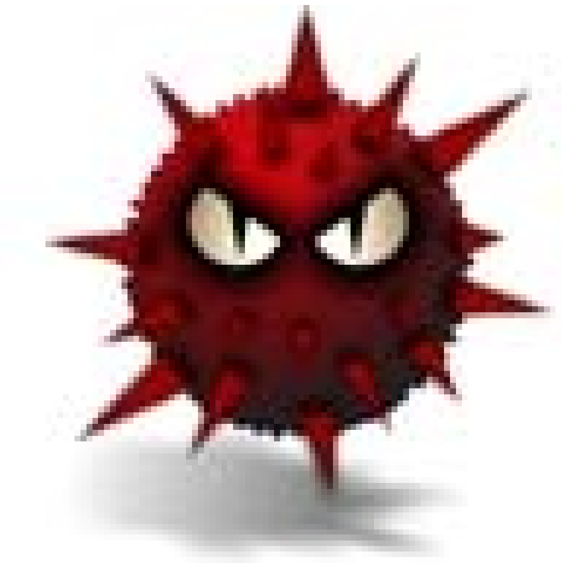
- Established in 2001
- 25 dedicated people
- Paris, Geneva, Montreal, Singapore

Our direct CSIRT-related activities for our constituency:

- Vulnerability Surveillance Service (Vulnerability Database and alerting)
- Cybercrime Surveillance and Analysis (Phishing, Malware, Studies)
- Emergency Response for Incidents

Introduction

PRG / NTOS / WSNPoem / Zbot / **ZeuS**



Anserin / **Torpig** / Sinowal / **Torpig Mebroot (MBR)**

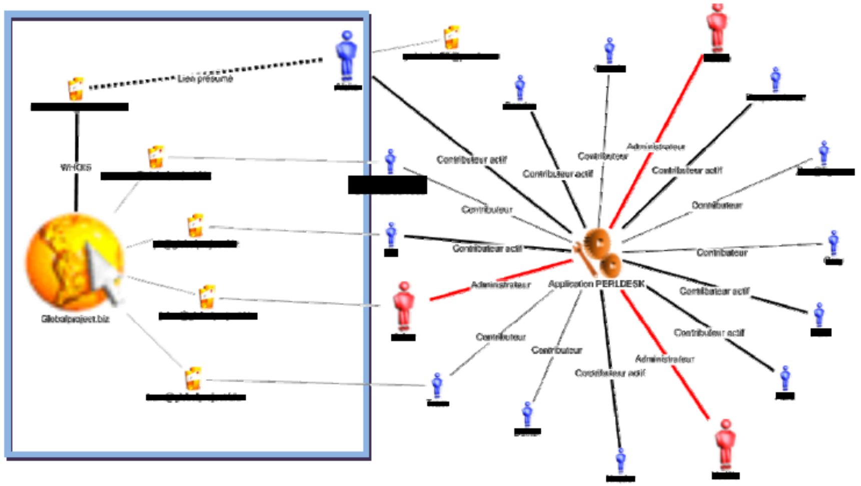
Ecosystems

Torpig ecosystem

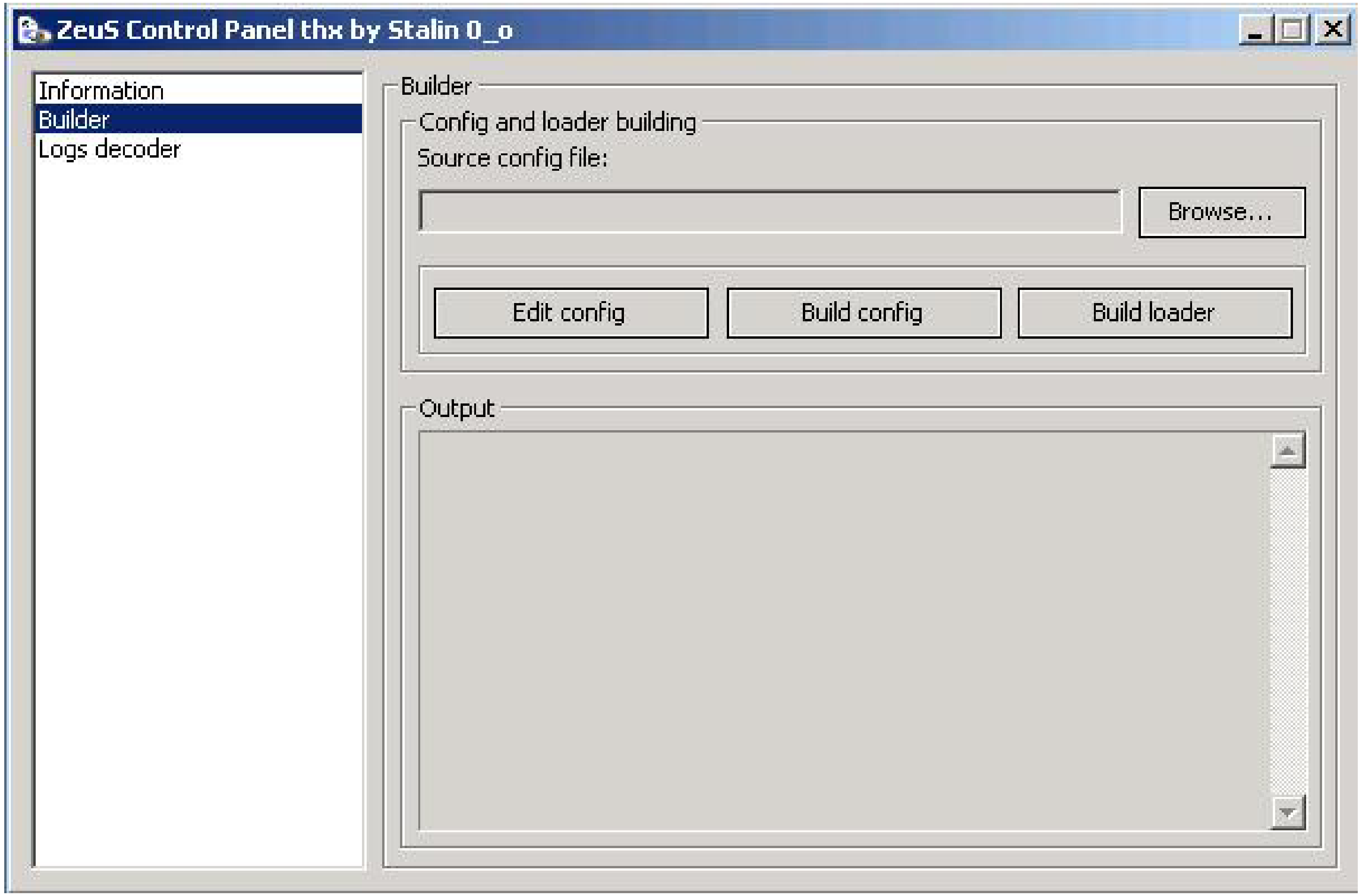
- Malware as a service (MaaS)
- Piloted by a few coders/administrators
- Selected clients (cooptation) that ensure propagation (15-20)
- Centralized data collection and dispatch to clients
- All private > no public offering

PRG ecosystem

- Malware kit is sold on black markets (Official price : 3000 USD)
- Probably 100+
- Bad support
- Models such as a311, haxdoor, Pinch…



PRG (ZeuS) Control Panel

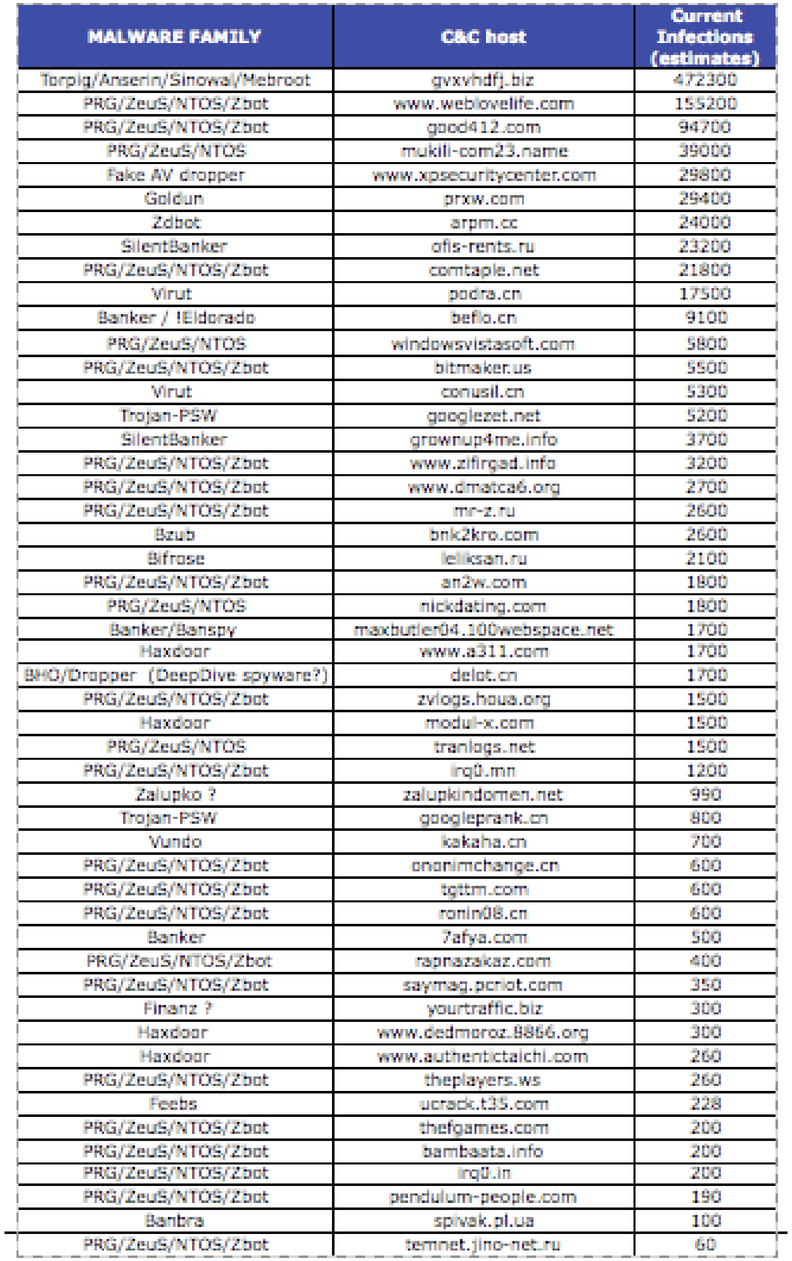


ZeuS Control Panel thx by Stalin 0_o

Propagation

Torpig propagation

- Drive-bys mainly, exploits kits (Neosploit)
- Today about 250k infections

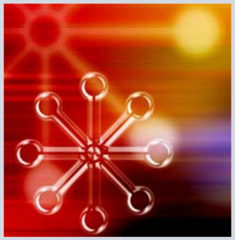


MALWARE FAMILY	C&C host	Current Infections (estimates)
Torpig/Anserin/Sinowal/Mebroot	gvxvhdfj.biz	472300
PRG/ZeuS/NTOS/Zbot	www.weblovelife.com	155200
PRG/ZeuS/NTOS/Zbot	good412.com	94700
PRG/ZeuS/NTOS	mukili-com23.name	39000
Fake AV dropper	www.xpsecuritycenter.com	29800
Goldun	prxw.com	29400
Zdbot	arpm.cc	24000
SilentBanker	ofis-rents.ru	23200
PRG/ZeuS/NTOS/Zbot	comtaple.net	21800
Virut	podra.cn	17500
Banker / !Eldorado	beflo.cn	9100
PRG/ZeuS/NTOS	windowsvistasoft.com	5800
PRG/ZeuS/NTOS/Zbot	bitmaker.us	5500
Virut	conusil.cn	5300
Trojan-PSW	googlezet.net	5200
SilentBanker	grownup4me.info	3700
PRG/ZeuS/NTOS/Zbot	www.zifirgad.info	3200
PRG/ZeuS/NTOS/Zbot	www.dmatca6.org	2700
PRG/ZeuS/NTOS/Zbot	mr-z.ru	2600
Bzub	bnk2kro.com	2600
Bifrose	leliksan.ru	2100
PRG/ZeuS/NTOS/Zbot	an2w.com	1800
PRG/ZeuS/NTOS	nickdating.com	1800
Banker/Banspy	maxbutler04.100webspace.net	1700
Haxdoor	www.a311.com	1700
BHO/Dropper (DeepDive spyware?)	delot.cn	1700
PRG/ZeuS/NTOS/Zbot	zvlogs.houa.org	1500
Haxdoor	modul-x.com	1500
PRG/ZeuS/NTOS	tranlogs.net	1500
PRG/ZeuS/NTOS/Zbot	irq0.mn	1200
Zalupko ?	zalupkindomen.net	990
Trojan-PSW	googleprank.cn	800
Vundo	kakaha.cn	700
PRG/ZeuS/NTOS/Zbot	ononimchange.cn	600
PRG/ZeuS/NTOS/Zbot	tgttm.com	600
PRG/ZeuS/NTOS/Zbot	ronin08.cn	600
Banker	7afya.com	500
PRG/ZeuS/NTOS/Zbot	rapnazakaz.com	400
PRG/ZeuS/NTOS/Zbot	saymag.pcriot.com	350
Finanz ?	yourtraffic.biz	300
Haxdoor	www.dedmoroz.8866.org	300
Haxdoor	www.authentictaichi.com	260
PRG/ZeuS/NTOS/Zbot	theplayers.ws	260
Feebs	ucrack.t35.com	228
PRG/ZeuS/NTOS/Zbot	thefgames.com	200
PRG/ZeuS/NTOS/Zbot	bambaata.info	200
PRG/ZeuS/NTOS/Zbot	irq0.in	200
PRG/ZeuS/NTOS/Zbot	pendulum-people.com	190
Banbra	spivak.pl.ua	100
PRG/ZeuS/NTOS/Zbot	temnet.jino-net.ru	60

PRG propagation

- Mail attachments, drive-bys , exploits kits (el fiesta)
- about 100-200k infections

Clients Code



Torpig / Mebroot Code

- Big evolutions: MBR Rootkit
- Strong skills, core injection, updated dlls
- Form-grabbing and injection
- Not for sell (service)
- Hard to Detect for Avs

PRG Code

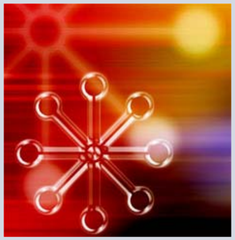
- No real evolution
- Userland, inject in processes
- Capacity for RT MitM
- For sell everywhere, kits disclosed
- Good AV coverage

```
 0:   fa                  cli
 1:   33 db               xor    bx,bx
 3:   8e d3               mov    ss,bx
 5:   36 89 26 fe 7b      mov    WORD PTR ss:0x7bfe,sp
 a:   bc fe 7b            mov    sp,0x7bfe
 d:   1e                  push   ds
 e:   66                  data32
 f:   60                  pusha
10:   fc                  cld
11:   8e db               mov    ds,bx
13:   be 13 04            mov    si,0x413
16:   83 2c 02            sub    WORD PTR [si],0x2
19:   ad                  lods   ax,WORD PTR ds:[si]
1a:   c1 e0 06            shl    ax,0x6
1d:   8e c0               mov    es,ax
```

CERT-LEXSI

LEXSI

Infrastructure



Torpig infrastructure

- One single c&c, rotating frequently
- c&c shutdown prevention
- Major variants now with MBR
- Multiple builds (clients)
- No bullet-proof hosting anymore
- Infrastructure strategy: be stealth, feed the beast.

PRG infrastructure

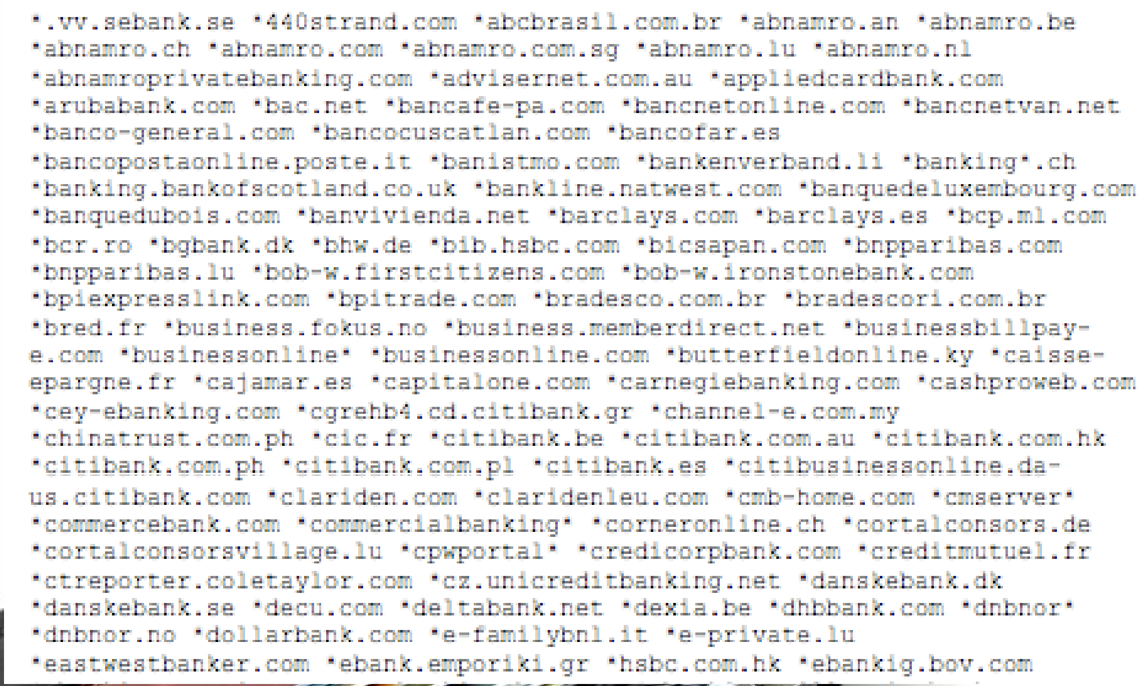
- Each client has its own infra
- Multiple variants as the kit is spread
- Some at bullet-proof hosting
- Infrastructure strategy: none

Torpig Targets

One unique Targets configuration file:

- 2,000+ targets

(now around 250)



```
*.vv.sebank.se *440strand.com *abcbrasil.com.br *abnamro.an *abnamro.be
*abnamro.ch *abnamro.com *abnamro.com.sg *abnamro.lu *abnamro.nl
*abnamroprivatebanking.com *advisernet.com.au *appliedcardbank.com
*arubabank.com *bac.net *bancafe-pa.com *bancnetonline.com *bancnetvan.net
*banco-general.com *bancocuscatlan.com *bancofar.es
*bancopostaonline.poste.it *banistmo.com *bankenverband.li *banking*.ch
*banking.bankofscotland.co.uk *bankline.natwest.com *banquedeluxembourg.com
*banquedubois.com *banvivienda.net *barclays.com *barclays.es *bcp.ml.com
*bcr.ro *bgbank.dk *bhw.de *bib.hsbc.com *bicsapan.com *bnpparibas.com
*bnpparibas.lu *bob-w.firstcitizens.com *bob-w.ironstonebank.com
*bpiexpresslink.com *bpitrade.com *bradesco.com.br *bradescori.com.br
*bred.fr *business.fokus.no *business.memberdirect.net *businessbillpay-
e.com *businessonline* *businessonline.com *butterfieldonline.ky *caisse-
epargne.fr *cajamar.es *capitalone.com *carnegiebanking.com *cashproweb.com
*cey-ebanking.com *cgrehb4.cd.citibank.gr *channel-e.com.my
*chinatrust.com.ph *cic.fr *citibank.be *citibank.com.au *citibank.com.hk
*citibank.com.ph *citibank.com.pl *citibank.es *citibusinessonline.da-
us.citibank.com *clariden.com *claridenleu.com *cmb-home.com *cmserver*
*commercebank.com *commercialbanking* *corneronline.ch *cortalconsors.de
*cortalconsorsvillage.lu *cpwportal* *credicorpbank.com *creditmutuel.fr
*ctreporter.coletaylor.com *cz.unicreditbanking.net *danskebank.dk
*danskebank.se *decu.com *deltabank.net *dexia.be *dhbbank.com *dnbnor*
*dnbnor.no *dollarbank.com *e-familybnl.it *e-private.lu
*eastwestbanker.com *ebank.emporiki.gr *hsbc.com.hk *ebankig.bov.com
```

CERT-LEXSI

LEXSI

PRG Targets

Analyzing 243 PRG unique configuration files

- 982 targeted domains
- very small overlap / never the exact same configuration files

fiducia.de	225
internetbanking.gad.de	219
vr-networld-ebanking.de	218
gruposantander.es	198
norisbank.de	197
comdirect.de	190
dresdner-privat.de	188
citibank.de	185
e-gold.com	182
bancajaproximaempresas.com	175
bankofamerica.com	174
chase.com	174
wellsfargo.com	171
paypal.com	165
banesto.es	164
osmp.ru	162
citibank.com	161
openbank.es	156
wamu.com	153
wachovia.com	153
lloydstsb.co.uk	150
ybonline.co.uk	150
halifax-online.co.uk	150
bancopopular.es	147
hsbc.co.uk	147
cajacanarias.es	146
lloydstsb.com	146
barclays.co.uk	145
cbonline.co.uk	143
caja-granada.es	143
clavenet.net	143
www.ccm.es	142
ccm.es	142
cajamadridempresas.es	137
cajabadajoz.es	136
nationalcity.com	136
unicaja.es	135
53.com	135
tdcanadatrust.com	134
citizensbankonline.com	134
usbank.com	133
suntrust.com	132
cajadeavila.es	131
quiubi.it	130
yandex.ru	130
isideonline.it	129
secservizi.it	128
iwbank.it	127
cajamadrid.es	127
bancopastor.es	127
rupay.com	127
poste.it	127
nwolb.com	127
cajamurcia.es	127
cajasoldirecto.es	126
bancaintesa.it	125
nationet.com	125
cajavital.es	124
uno-e.com	124
banif.es	124
bgnetplus.com	123
co-operativebank.co.uk	122
caixatarragona.es	122
caixagirona.es	122
smile.co.uk	122
bbvanetoffice.com	121
fibancmediolanum.es	121
sabadellatlantico.com	121
caixalaietana.es	120
barclays.com	120
banquepopulaire.fr	120
cajaen.es	119
hsbc.com	117
webmoney.ru	117
caixaontinyent.es	117
cajarioja.es	116
elmonte.es	116
gruppocarige.it	115
cajacirculo.es	114
rbsdigital.com	112
…	

CERT-LEXSI

LEXSI

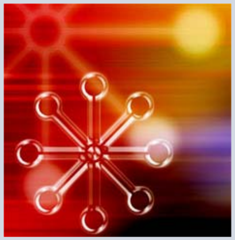
Cybercriminal’s Torpig short analysis

⊕	Hard to catch (private ring) Money goes to coders Understand payment interfaces Find channels for monetizing
⊖	Loss of opportunities Centralized head Predictable c&c

Cybercriminal’s PRG short analysis

⊕	Less expensive No predictable c&c
⊖	Easy to catch (public ring) Not a really “malware as a service”

Comparison and efficiency



Look-a-likes

- Similar objectives: money
- Similar interception methods
- Both Russian-speaking ring

Differences

- in code skills
- in infrastructure protection
- in private/public market approach

Thank you

Any questions ?

- Thomas GAYET - Speaker
- Vincent HINDERER

- cert@lexsi.com
- http://cert.lexsi.com/