Cyber Crime,
Data Breaches,
Mobile Technology:
The Risks

PRIVACY AND CYBER CRIME INSTITUTE

RYERSON UNIVERSITY

Cyber Crime Trends

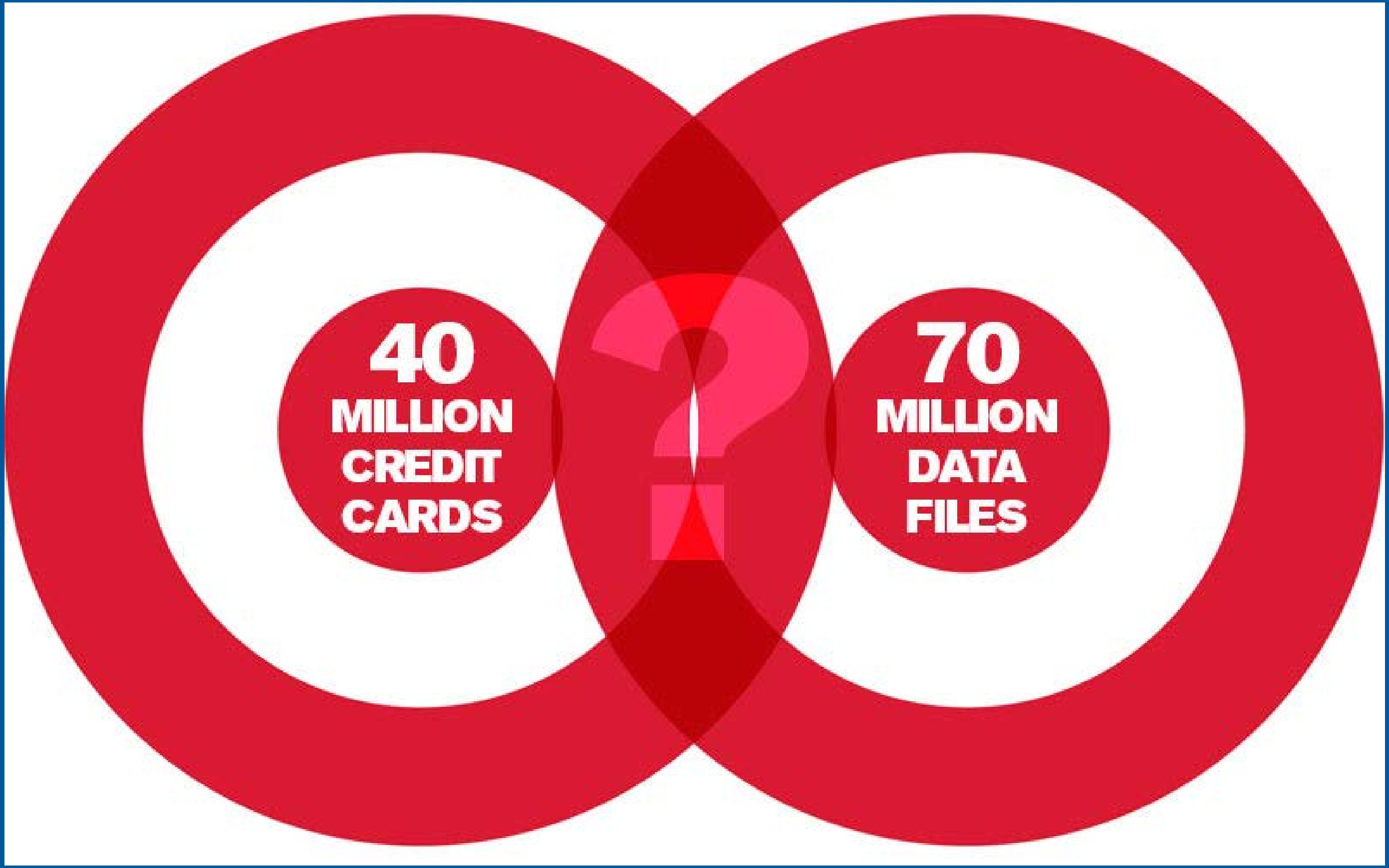
- War
  - – Shadowed by international conflict

Global Crime

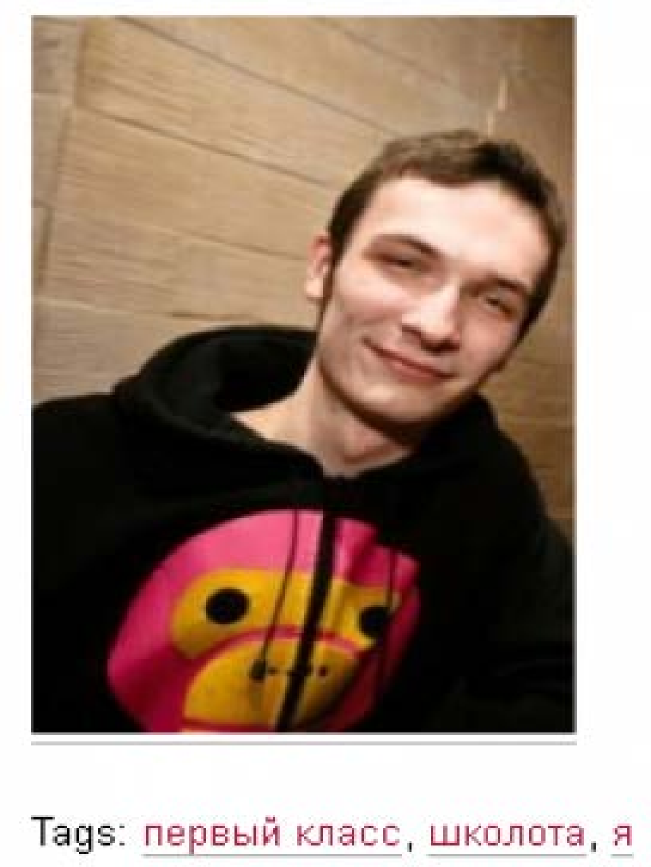
- Originates outside jurisdiction
- Difficult for LEAs to coordinate
- Time and resource consuming

Gameover ZeuS Botnet

Target Breach



Target Suspect

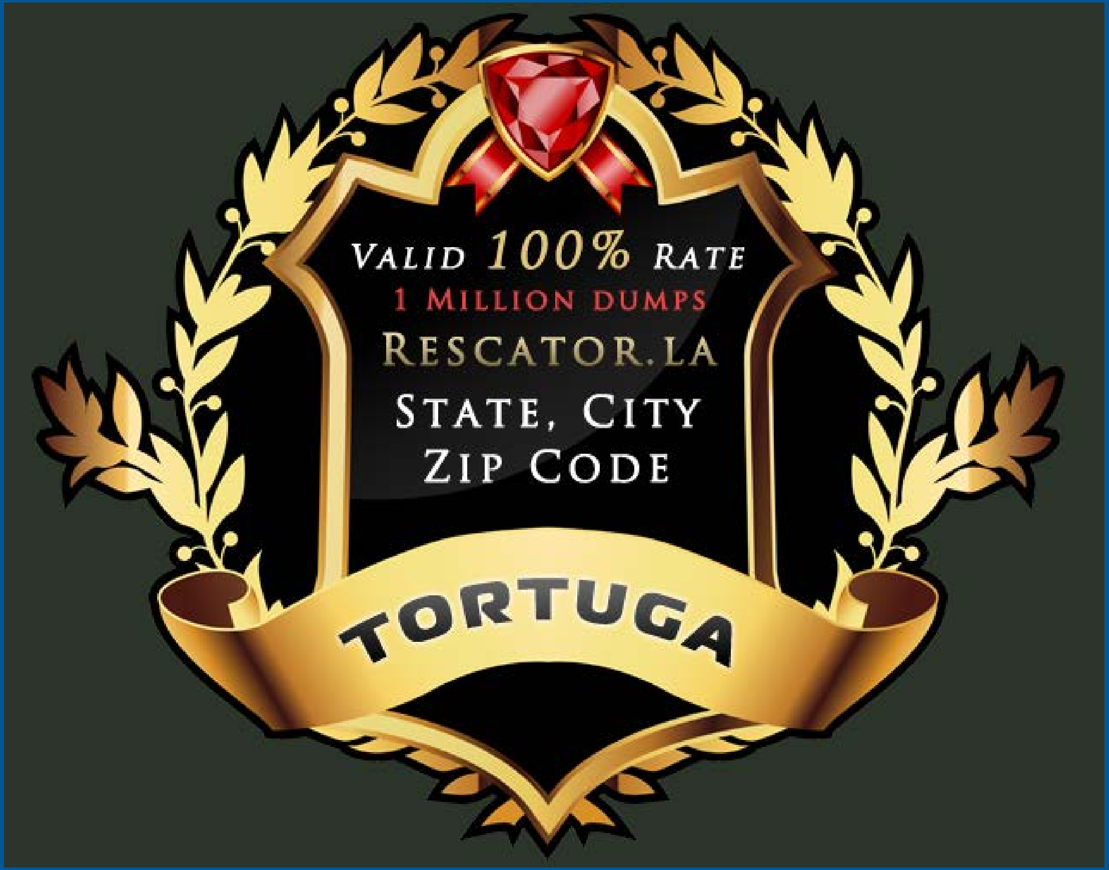


Tags: первый класс, школота, я

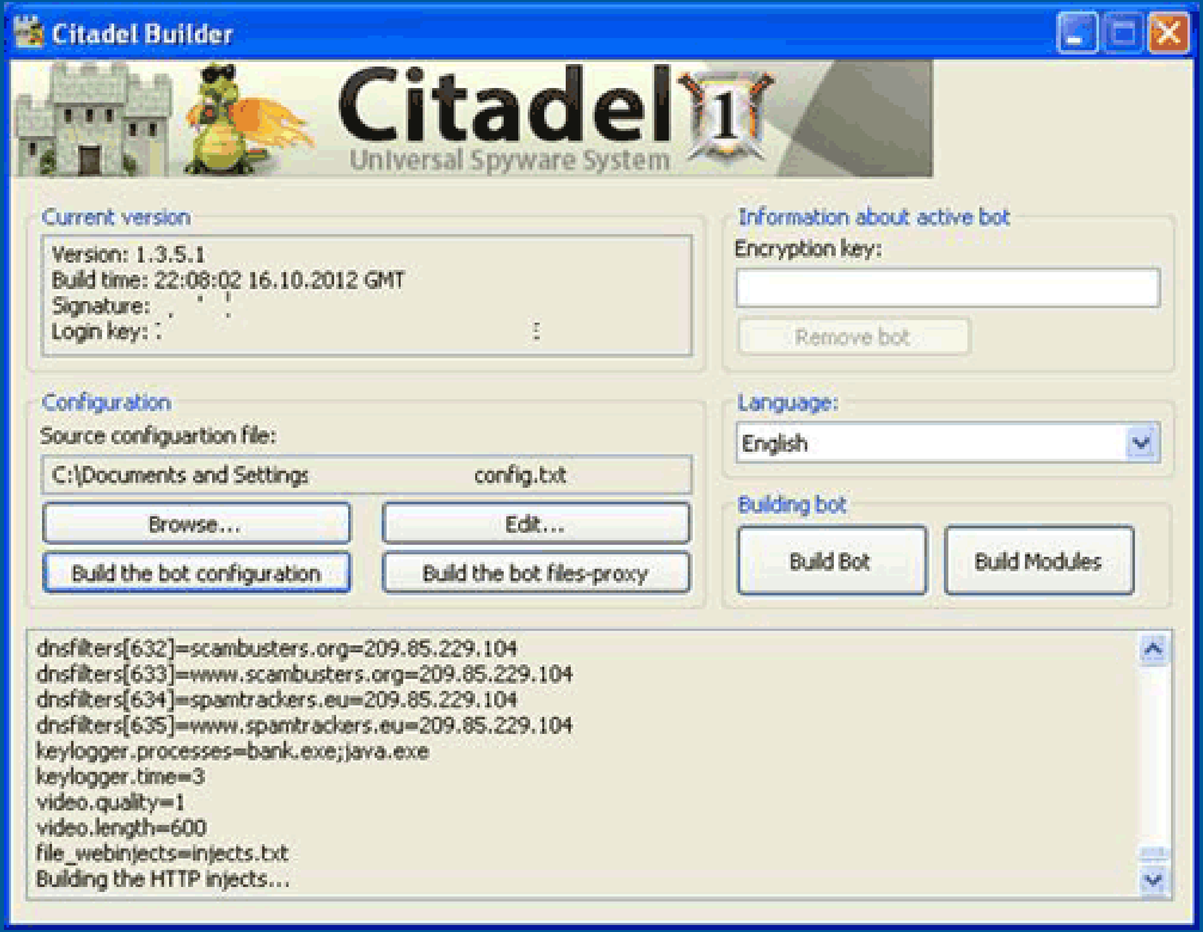
Crime as Retail

- Supply chains
  - – Proceeds
  - – Tools
- Lay end-users
  - – “consumers” not “manufacturers”

Proceeds Chain



Tool Chain



Current version

Version: 1.3.5.1
Build time: 22:08:02 16.10.2012 GMT
Signature:
Login key:

Information about active bot

Encryption key:

Configuration

Source configuartion file:

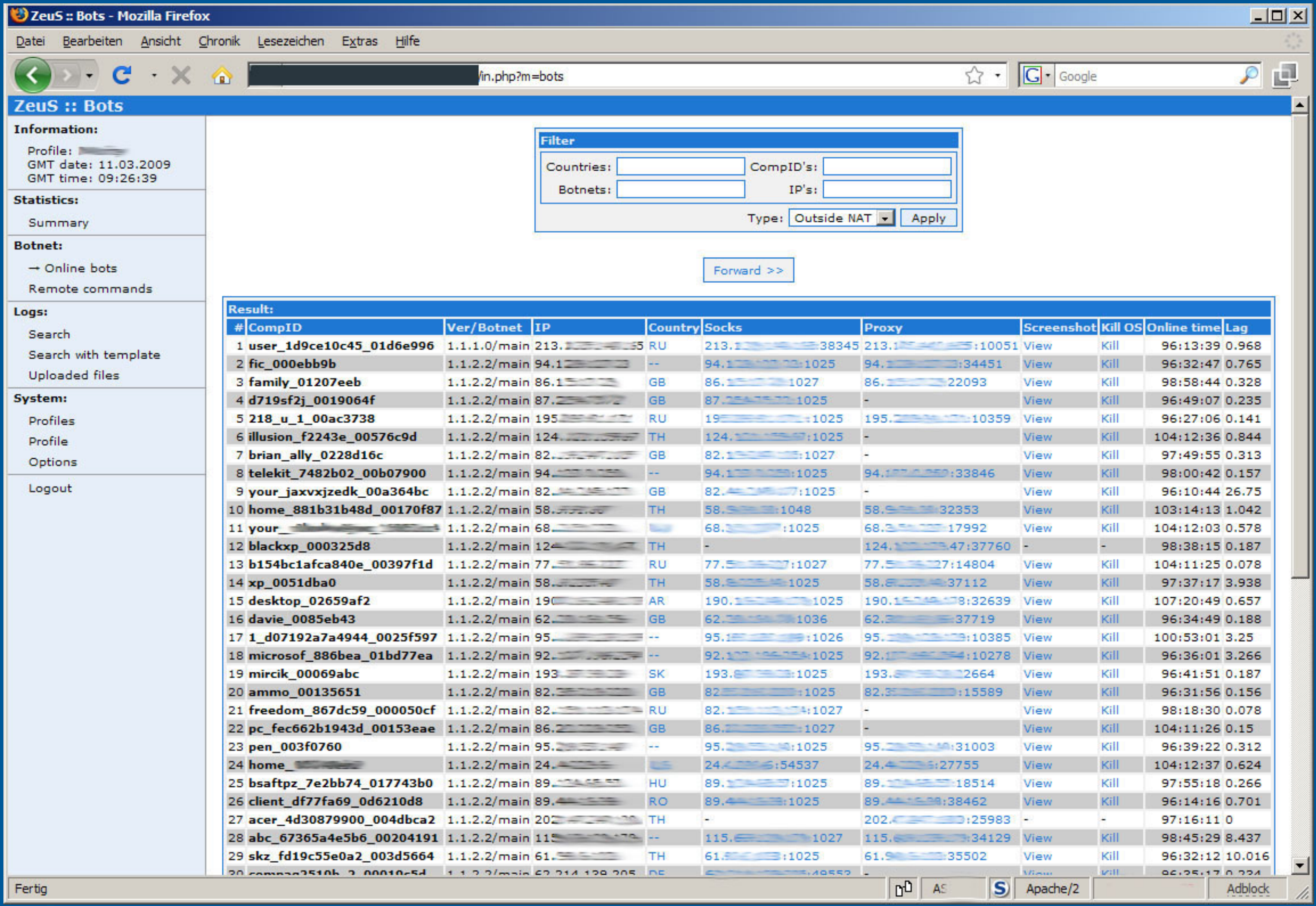
C:\Documents and Settings config.txt

Language: English

Building bot

```
dnsfilters[632]=scambusters.org=209.85.229.104
dnsfilters[633]=www.scambusters.org=209.85.229.104
dnsfilters[634]=spamtrackers.eu=209.85.229.104
dnsfilters[635]=www.spamtrackers.eu=209.85.229.104
keylogger.processes=bank.exe;java.exe
keylogger.time=3
video.quality=1
video.length=600
file_webinjects=injects.txt
Building the HTTP injects...
```

Zeus Interface



ZeuS :: Bots - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Google

[redacted]/in.php?m=bots

ZeuS :: Bots

Information:
Profile: [redacted]
GMT date: 11.03.2009
GMT time: 09:26:39

Statistics:
Summary

Botnet:
→ Online bots
Remote commands

Logs:
Search
Search with template
Uploaded files

System:
Profiles
Profile
Options

Logout

Filter

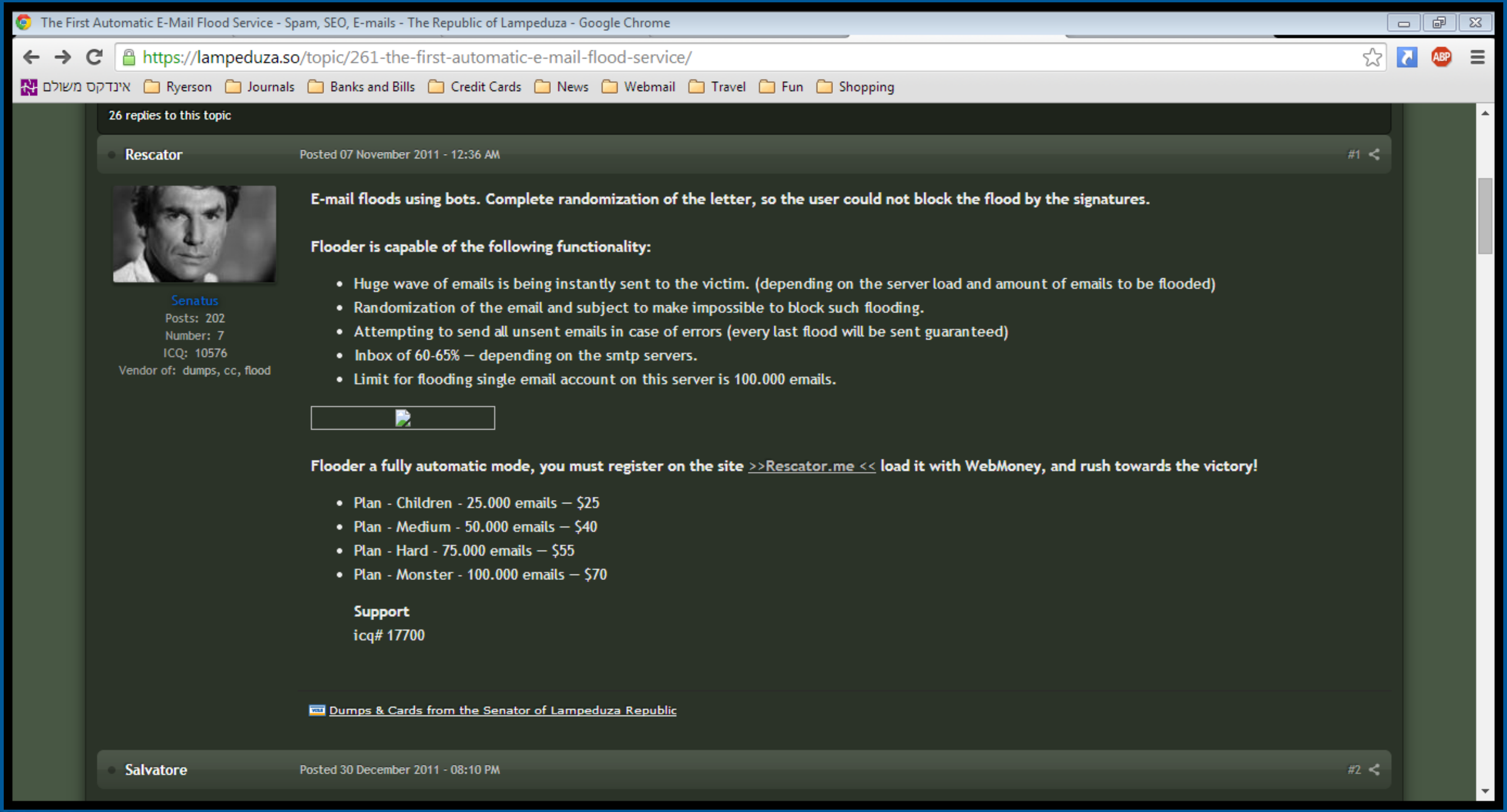
Countries: ____ CompID's: ____
Botnets: ____ IP's: ____
Type: Outside NAT [Apply]

[Forward >>]

Result:

#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Kill OS	Online time	Lag
1	user_1d9ce10c45_01d6e996	1.1.1.0/main	213.[redacted]5	RU	213.1[redacted]38345	213.1[redacted]:10051	View	Kill	96:13:39	0.968
2	fic_000ebb9b	1.1.2.2/main	94.1[redacted]	--	94.1[redacted]:1025	94.[redacted]:34451	View	Kill	96:32:47	0.765
3	family_01207eeb	1.1.2.2/main	86.1[redacted]	GB	86.[redacted]1027	86.[redacted]22093	View	Kill	98:58:44	0.328
4	d719sf2j_0019064f	1.1.2.2/main	87.[redacted]	GB	87.[redacted]1025	-	View	Kill	96:49:07	0.235
5	218_u_1_00ac3738	1.1.2.2/main	195[redacted]	RU	19[redacted]:1025	195.[redacted]10359	View	Kill	96:27:06	0.141
6	illusion_f2243e_00576c9d	1.1.2.2/main	124.[redacted]	TH	124.[redacted]:1025	-	View	Kill	104:12:36	0.844
7	brian_ally_0228d16c	1.1.2.2/main	82.[redacted]	GB	82.1[redacted]:1027	-	View	Kill	97:49:55	0.313
8	telekit_7482b02_00b07900	1.1.2.2/main	94.[redacted]	--	94.1[redacted]:1025	94.[redacted]:33846	View	Kill	98:00:42	0.157
9	your_jaxvxjzedk_00a364bc	1.1.2.2/main	82.[redacted]	GB	82.[redacted]:1025	-	View	Kill	96:10:44	26.75
10	home_881b31b48d_00170f87	1.1.2.2/main	58.[redacted]	TH	58.[redacted]:1048	58.[redacted]32353	View	Kill	103:14:13	1.042
11	your_[redacted]	1.1.2.2/main	68.[redacted]	[redacted]	68.[redacted]:1025	68.[redacted]17992	View	Kill	104:12:03	0.578
12	blackxp_000325d8	1.1.2.2/main	12[redacted]	TH	-	124.[redacted].47:37760	-	-	98:38:15	0.187
13	b154bc1afca840e_00397f1d	1.1.2.2/main	77.[redacted]	RU	77.[redacted]:1027	77.[redacted]27:14804	View	Kill	104:11:25	0.078
14	xp_0051dba0	1.1.2.2/main	58.[redacted]	TH	58.[redacted]1025	58.[redacted]37112	View	Kill	97:37:17	3.938
15	desktop_02659af2	1.1.2.2/main	190[redacted]	AR	190.1[redacted]1025	190.1[redacted]8:32639	View	Kill	107:20:49	0.657
16	davie_0085eb43	1.1.2.2/main	62.[redacted]	GB	62.[redacted]1036	62.[redacted]37719	View	Kill	96:34:49	0.188
17	1_d07192a7a4944_0025f597	1.1.2.2/main	95.[redacted]	--	95.1[redacted]:1026	95.[redacted]:10385	View	Kill	100:53:01	3.25
18	microsof_886bea_01bd77ea	1.1.2.2/main	92.[redacted]	--	92.1[redacted]1025	92.1[redacted]:10278	View	Kill	96:36:01	3.266
19	mircik_00069abc	1.1.2.2/main	193[redacted]	SK	193.[redacted]:1025	193.[redacted]2664	View	Kill	96:41:51	0.187
20	ammo_00135651	1.1.2.2/main	82.[redacted]	GB	82[redacted]:1025	82.3[redacted]:15589	View	Kill	96:31:56	0.156
21	freedom_867dc59_000050cf	1.1.2.2/main	82.[redacted]	RU	82.1[redacted]:1027	-	View	Kill	98:18:30	0.078
22	pc_fec662b1943d_00153eae	1.1.2.2/main	86.[redacted]	GB	86.[redacted]:1027	-	View	Kill	104:11:26	0.15
23	pen_003f0760	1.1.2.2/main	95.[redacted]	--	95.[redacted]:1025	95.[redacted]:31003	View	Kill	96:39:22	0.312
24	home_[redacted]	1.1.2.2/main	24.[redacted]	[redacted]	24.[redacted]:54537	24.[redacted]:27755	View	Kill	104:12:37	0.624
25	bsaftpz_7e2bb74_017743b0	1.1.2.2/main	89.[redacted]	HU	89.[redacted]:1025	89.[redacted]18514	View	Kill	97:55:18	0.266
26	client_df77fa69_0d6210d8	1.1.2.2/main	89.[redacted]	RO	89.[redacted]:1025	89.[redacted]:38462	View	Kill	96:14:16	0.701
27	acer_4d30879900_004dbca2	1.1.2.2/main	20[redacted]	TH	-	202.[redacted]:25983	-	-	97:16:11	0
28	abc_67365a4e5b6_00204191	1.1.2.2/main	11[redacted]	--	115.[redacted]1027	115.[redacted]:34129	View	Kill	98:45:29	8.437
29	skz_fd19c55e0a2_003d5664	1.1.2.2/main	61.[redacted]	TH	61.[redacted]:1025	61.[redacted]35502	View	Kill	96:32:12	10.016
30	compaq2510b_2_00010c5d	1.1.2.2/main	62.214.139.205	DE	[redacted]:49552	-	View	Kill	96:25:17	0.224

Email Tool


The First Automatic E-Mail Flood Service - Spam, SEO, E-mails - The Republic of Lampeduza - Google Chrome
https://lampeduza.so/topic/261-the-first-automatic-e-mail-flood-service/
אינדקס משולם
Ryerson
Journals
Banks and Bills
Credit Cards
News
Webmail
Travel
Fun
Shopping
ABP

26 replies to this topic

Rescator Posted 07 November 2011 - 12:36 AM #1

Senatus
Posts: 202
Number: 7
ICQ: 10576
Vendor of: dumps, cc, flood

E-mail floods using bots. Complete randomization of the letter, so the user could not block the flood by the signatures.

Flooder is capable of the following functionality:

- Huge wave of emails is being instantly sent to the victim. (depending on the server load and amount of emails to be flooded)
- Randomization of the email and subject to make impossible to block such flooding.
- Attempting to send all unsent emails in case of errors (every last flood will be sent guaranteed)
- Inbox of 60-65% – depending on the smtp servers.
- Limit for flooding single email account on this server is 100.000 emails.

Flooder a fully automatic mode, you must register on the site >>Rescator.me << load it with WebMoney, and rush towards the victory!

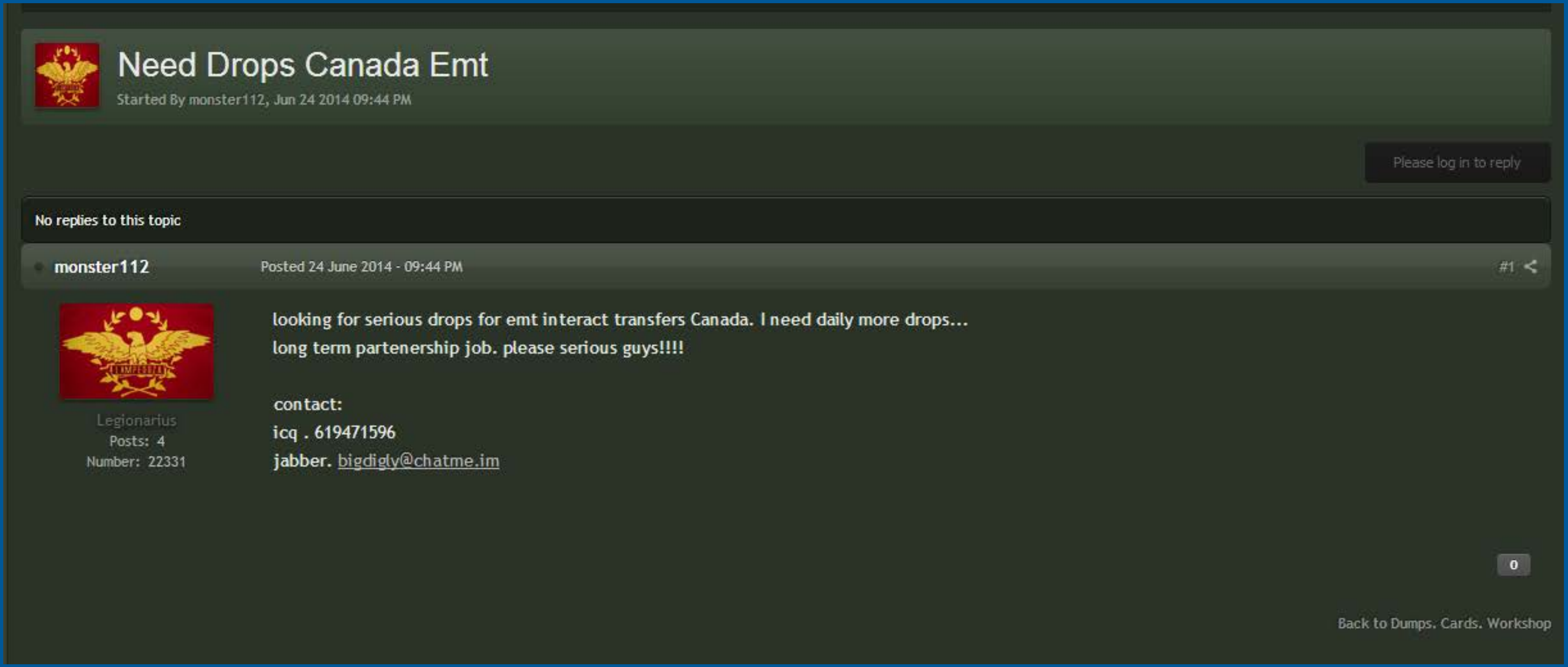
- Plan - Children - 25.000 emails – $25
- Plan - Medium - 50.000 emails – $40
- Plan - Hard - 75.000 emails – $55
- Plan - Monster - 100.000 emails – $70

Support
icq# 17700

Dumps & Cards from the Senator of Lampeduza Republic

Salvatore Posted 30 December 2011 - 08:10 PM #2

The latest…



Need Drops Canada Emt

Started By monster112, Jun 24 2014 09:44 PM

No replies to this topic

monster112 Posted 24 June 2014 - 09:44 PM #1

Legionarius
Posts: 4
Number: 22331

looking for serious drops for emt interact transfers Canada. I need daily more drops...
long term partenership job. please serious guys!!!!

contact:
icq . 619471596
jabber. bigdigly@chatme.im

Data Breach Implications

- Target – watershed
- Pre-target: no consequence
- Post-target: C-Suite
- Did Target have CISO?

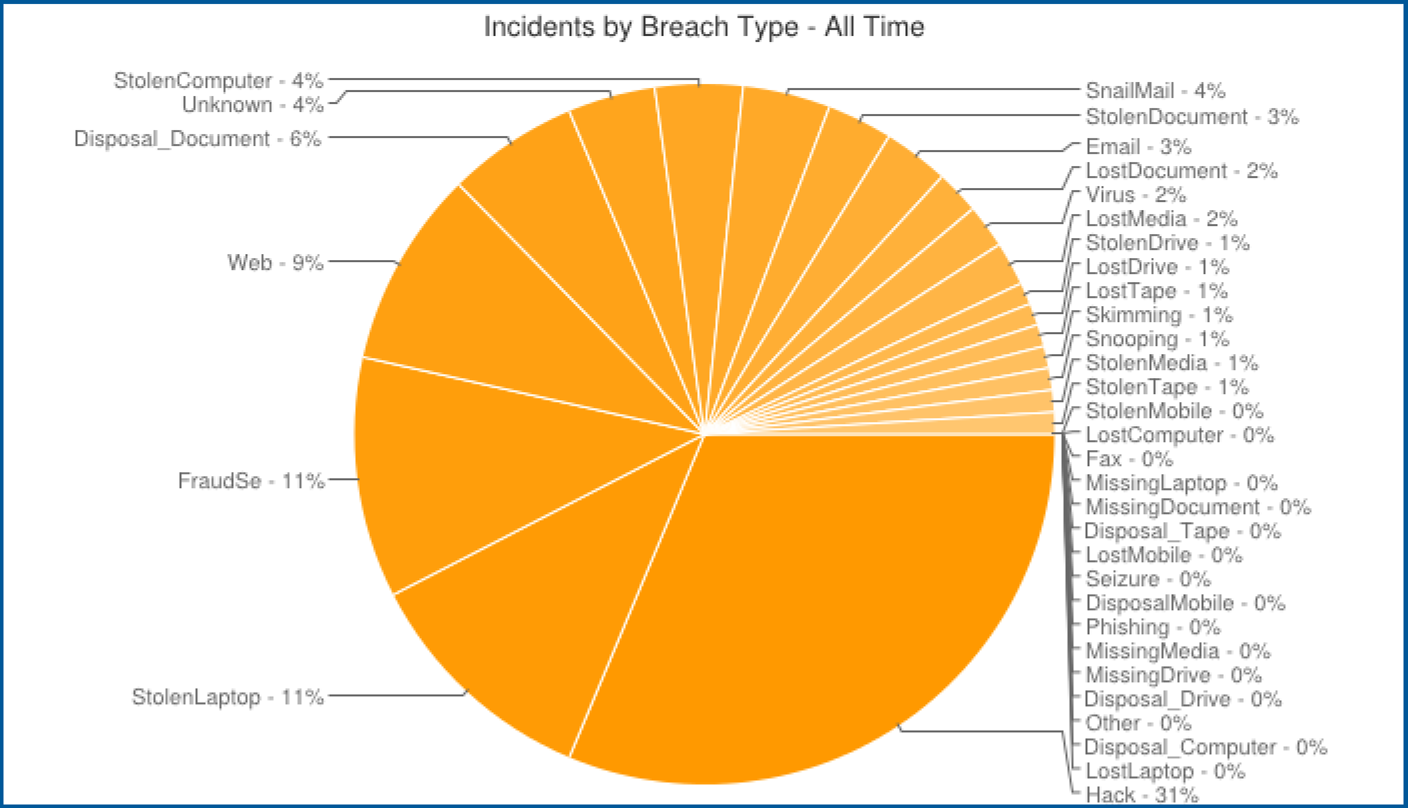
Canadian Landscape

- Federal Mandatory notification arriving
- Provincial – only Alberta
- Corporate discretion
- No role for regulator (OPC)

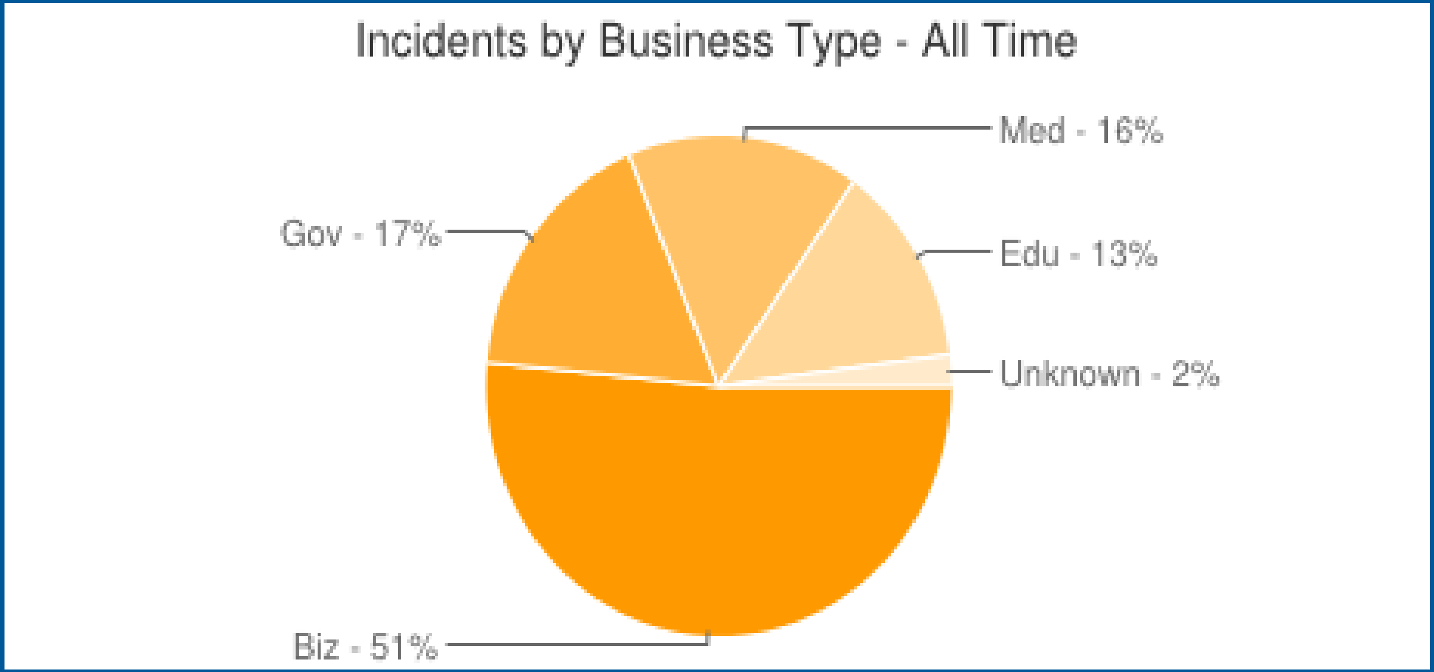
No Data

- Closely guarded
- No aggregation
- No public policy debate
- Extrapolation and guess-timates
- From $10 to $400 (million)
- 0.2% of GDP ~ $3.1 (billion)

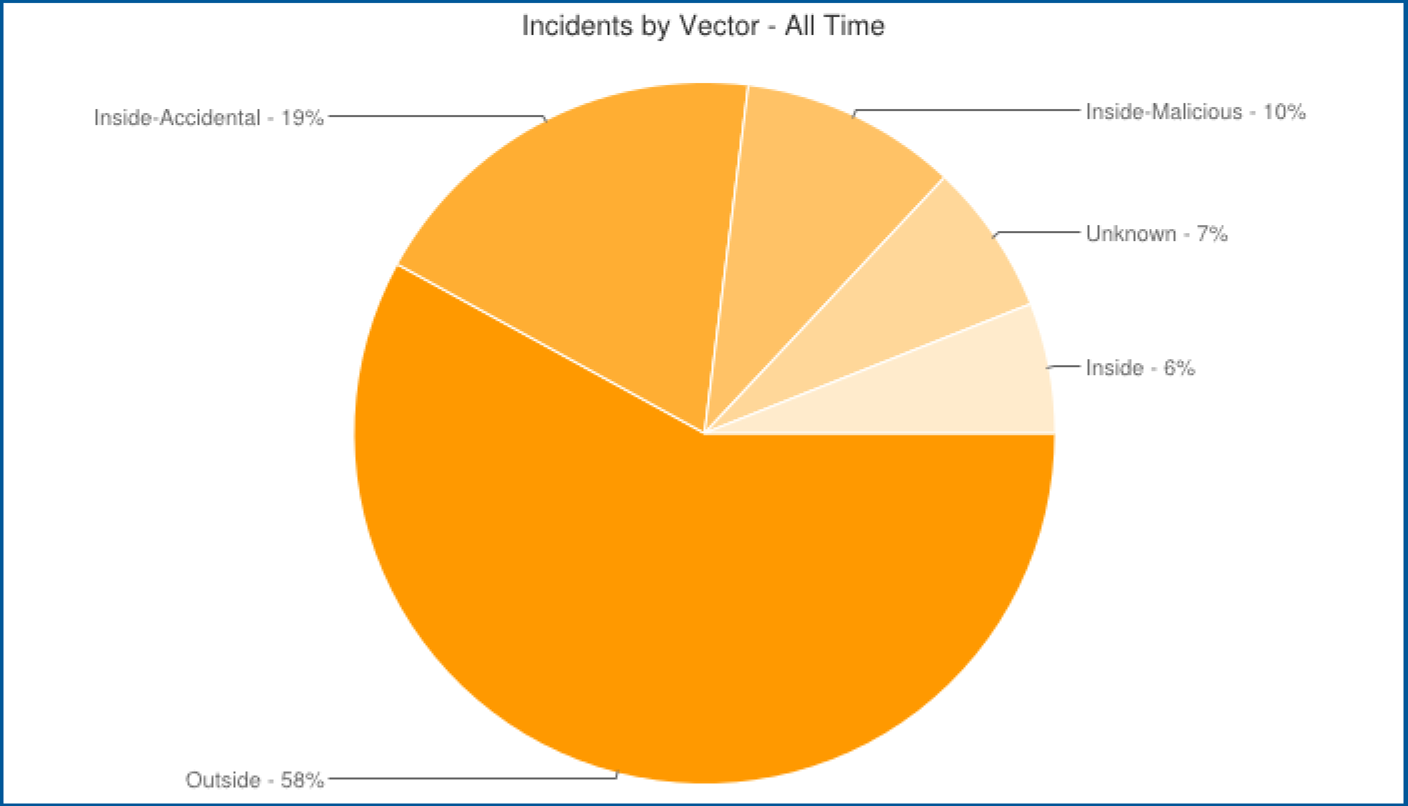
From Data Loss DB



Who is attacked



How they are attacked



Mobile Examples

Waller Trojan

What mal-apps do

- Pay-to-download
  - App triggers paid downloads
- Exploit digital wallets
  - Most concerning
- Other data mining
  - phone calls
  - contact list
  - geo-locations
  - text messages

Current Primary Risks

- Laptops
  - data and gateway
- Tablets
  - gateway
- Phones
  - gateway
- Sticks
  - data

Personal Use Risk

- BYOD
  - Can’t dictate platform (C-suite at fault)
- Credentials
  - Personal information
  - Social engineering
- Tinkering
  - Rooting
  - Third Party stores

Mobile Risk Management

- MDM
  - Sandboxing
- Insurance
  - Not a solution
- Minimal Security
  - Two factors
  - Passwords

Thank You

For Further Information:

http://www.ryerson.ca/privacyinstitute

privacy@ryerson.ca