RBNexploit.com

KEEPING AN EYE ON THE RUSSIAN BUSINESS NETWORK

Tracking the Russian Business Network (RBN)

Knowing and understanding the RBN is a useful objective,

but surely the main goal is to stop them?

By

Jart Armin

et. al

Background

Steve Gibson's keynote Anti-Spyware Coalition's annual public workshop Jun 07 says it all;

"***Really, the way we see this problem needs to change. We need to take proactive actions against bot networks. We need research to set up honeypots, get infected, and trace back to the botnet masters. Right now, we're being too reactive, and we need to become more proactive.***"

- Wikipedia and a blog (RBNexploit.blogspot.com)
- Jart, et .al ? – US, UK, FR, BE, CN, DE, RU, IN, UA, SE
- David Bizeul – RBN Study (FR)
- InfoSec community, Journalists
- Searching for Evil – Prof Ross Anderson & Dr. Richard Clayton

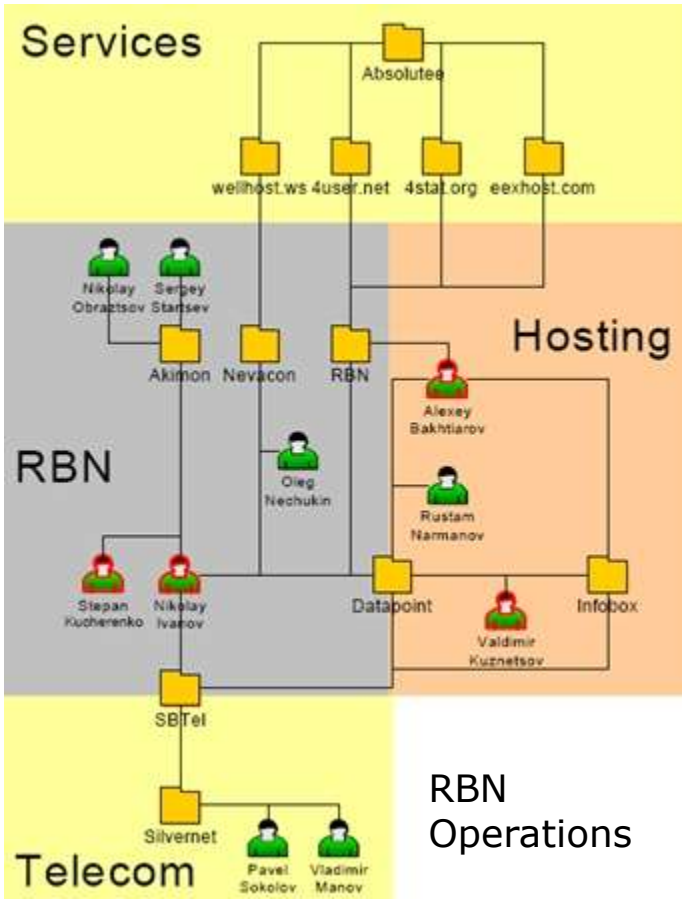
Introduction:

- Tracking the RBN – why?
- RBN – The Usual Suspects – Keyser Soze = RBN the Internet's bogey man? – Hiding from us or are we hiding from them?
- RBN - Deception and the art of "fear"
- RBN - Ghost in the machine (the case of Monster.com)
- Linguistics
- Law enforcement – Prevention or arrests?
- How to stop or can we?

RBN – Who?

12 Levashovskiy Prospect.
197110 Saint-Petersburg, - RU

Ref: Bizeul.org - 11/21/07



RBN Operations

Ref: Bizeul.org - 11/21/07

RBN – What? (a)

- The Russian Business Network (commonly abbreviated as RBN) is a Russian Internet Service Provider based in St. Petersburg which is notorious for its hosting of illegal and dubious businesses, including; child pornography, phishing and malware distribution sites. - Wikipedia

RBN – What? (b)

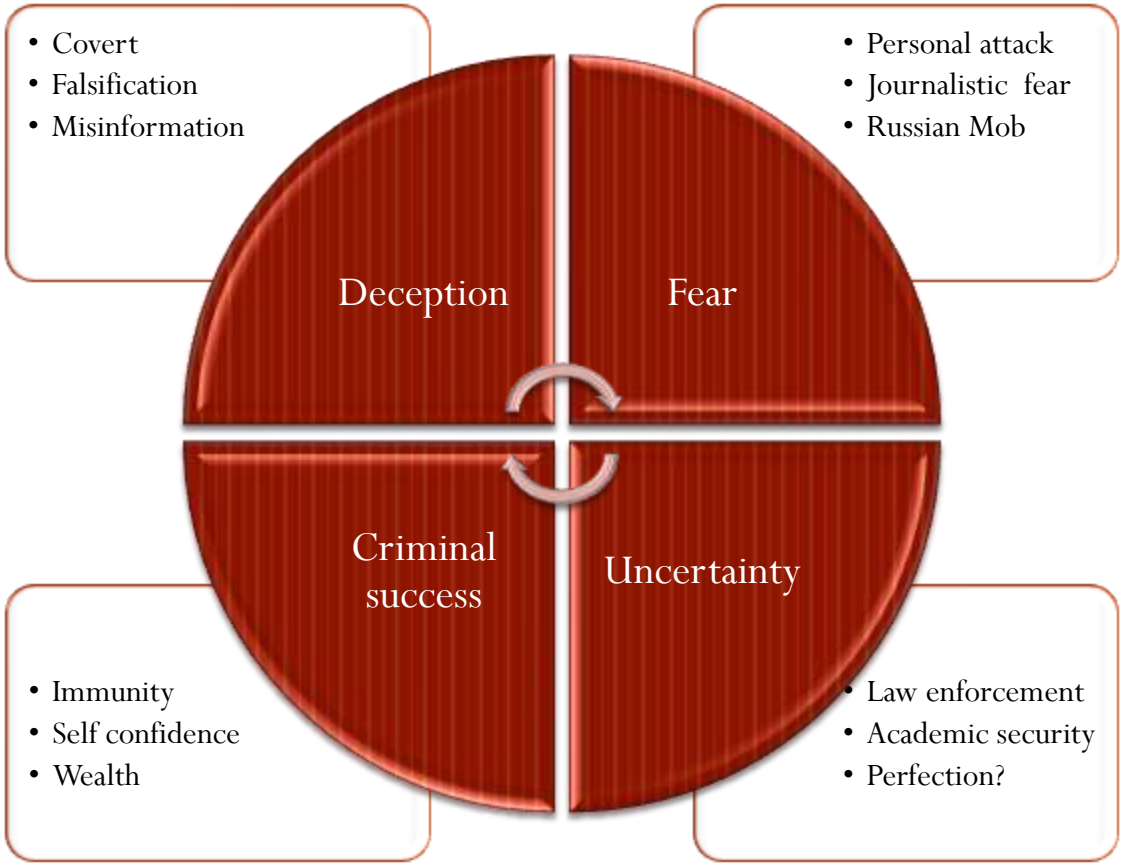
- The RBN is a multi-faceted criminal based internet business, specializing in and in some cases monopolizing personal identity theft for resale and exploitation. It also manages internet services for child pornography, spam, botnets, and malware distribution. The RBN's physical beginnings were from St. Petersburg Russia but now makes use of partner and affiliate marketing techniques in several countries to provide a method for organized crime to target victims internationally.

RBN – What? (c)

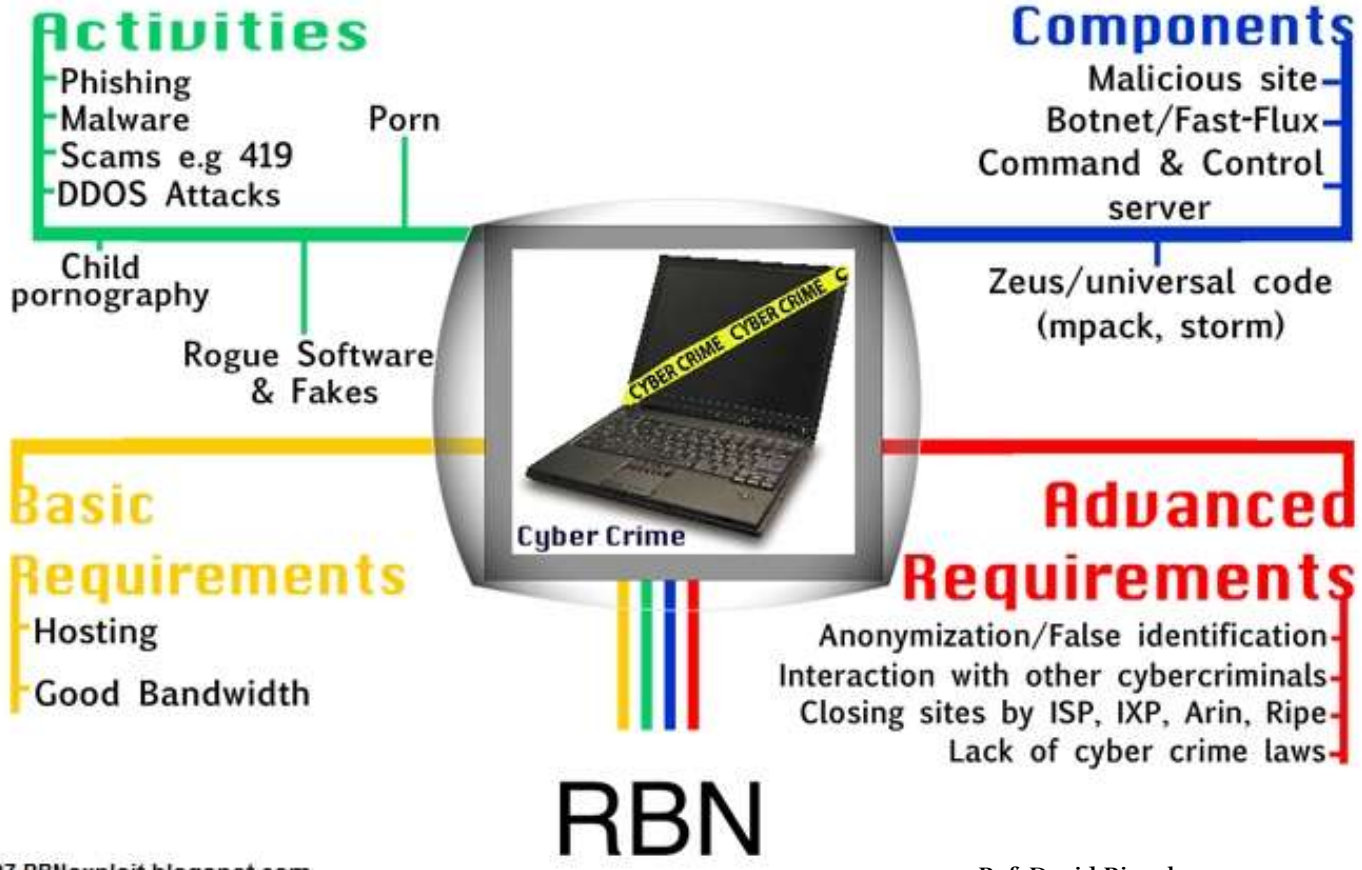
- RBN = bunch of web savvy, well organized confidence tricksters, thieves and crackers. Responsible for 60% of online crime. Stealing and profiting from Internet user's personal information.

  Tabloid version – avoid mythologizing – the RBN is not Keyser Soze, e.g. in Russia, hackers and RBN are generally considered as folk heroes screwing rich and fat westerners out of ill gotten gains.

RBN - Deception and the cycle of "fear"

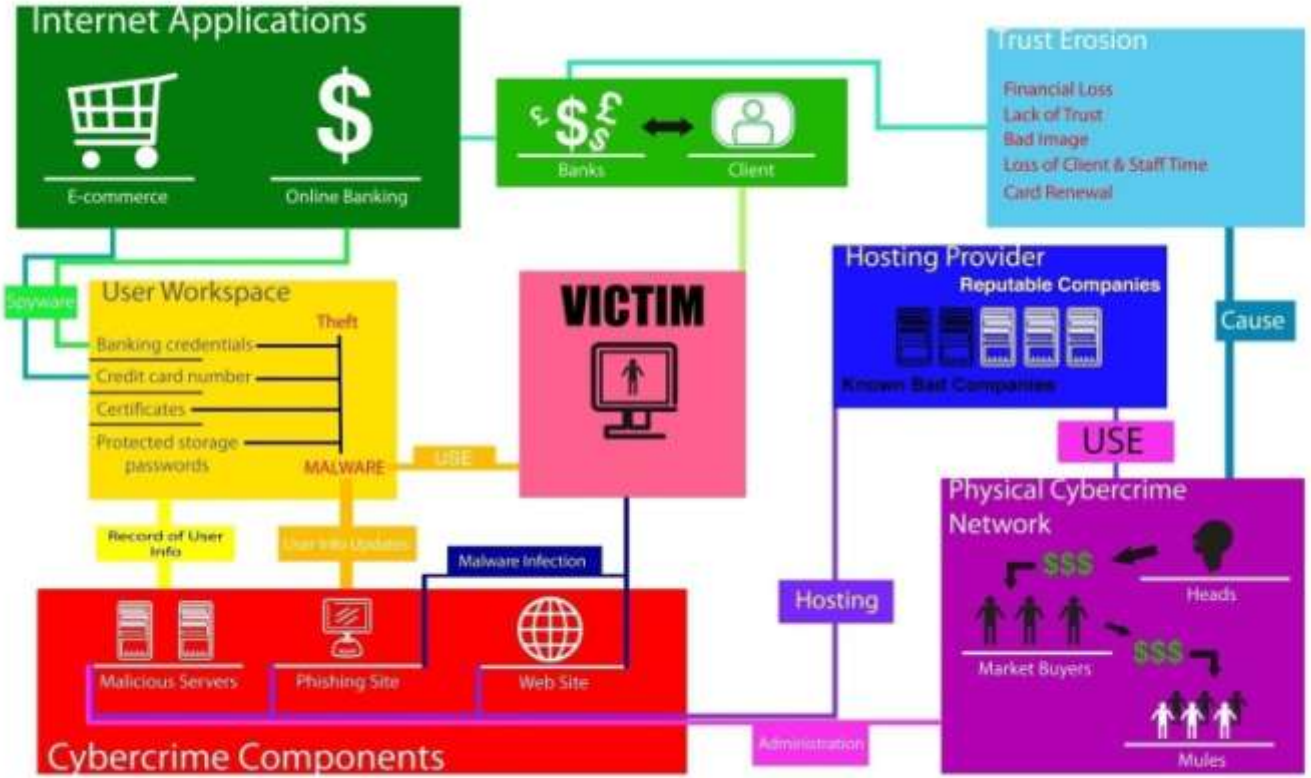


Requirements Model



Ref: David Bizeul

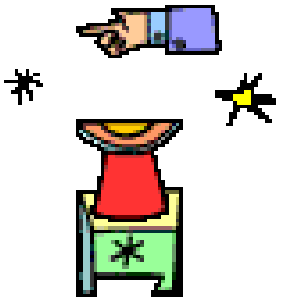
Process Model - Victim



Ref: David Bizeul

RBN – Purpose and attack vectors

One word = Fake!



- Occam's Razor – simplest solution is closest to the truth.
- Primarily the RBN's objective to use any and many alternative means to infect a PC and then gain or extort personal information, and if possible hijack / enslave the PC as zombie.

RBN = Fakes (1)

- Fake – anti-virus / anti-spyware web sites and products – try for free, get your PC really infected, and buy the solution from them, even if you do not buy the "fake" they have already stolen your personal ID.

- Fake – PC video codec web sites and products - try for free, get your PC really infected, and buy the solution from them to solve the problem they cause, and become a zombie.

- Fake – Advertising from "Double-Click" on large Internet portal web sites - recently; The Economist, MLB (baseball), NFL (ice hockey), CNN, etc. The ads had iFrame injections within to redirect the web site visitor's Internet browser to fake anti-virus / codec sites.

RBN = Fakes (2)

- Fake – Bank emails for phishing personal bank ID information (Rock Phish; Bank of India Hack, Australian bank, and others).

- Fake – Legitimate administrator access to web servers, web sites and web forums to inject malware into multiple web pages (e.g. 10,000 web sites on iPower web servers, 15,000 plus web sites on Italian web servers (Gromozon)

RBN = Fakes (3)

- Fake – Job opportunities / offers by email phishing for personal ID (Monster and CareerBuilder hacks)
- Fake – Data encryption, only after a payment is made can you unencrypt your data, and risk further ID theft (Ransom ware)
- Fake – Web search items in an attempt to direct a web surfer to an exploit based web page (Google).

Linguistics – defining the problem

Ethnomethodological approach:

- Seek to describe the practices and the methods the RBN uses in their actual descriptions of those settings.
- A research approach that describes the social practices ("methods") of its research subjects without the commonly accepted practice of evaluating the validity of those practices from an imposed normative standpoint.

Ghost in the machine

Words, words, words .....

- MPack
- IcePack
- Storm
- Torpig/Anserin/Sinowal, Briz, Haxdoor, Gozi/Banksniff
- Gromozon, Zlob
- Universal code, ZeuS, Zhelatin, Warezov, Bancos aam, Bzub, Gpcode ai

All "BadWare" – polymorphic soon?

Ghost in the machine– Monster.com

The example of the "ongoing" RBN managed attack on Monster.com, CareerBuilder.com and similar.

- Obviously a bad ID theft hack and phishing in itself, 2.4 million+ (known of) personal credentials stolen.
- A proportion of the credentials stolen are those technical personnel already within governmental law enforcement organizations or applying for such positions
- To be realistic do we think that a few of those individuals could not be personally compromised or bribed to divulge access information?
- Try this within your organization (examples gained a 20% bad response) . Approach a few of your lower level technical employees as an outsider with say a 250,000 Euro "cash" offer for network access details, how many would accept?

Law Enforcement

- The burglary analogy
- Research - Help or hinder?
- Law enforcement's response to research (-ve to +ve)
- Insurance, the missing link? (HK marine - COMINT)
- Speed of response, 3-4 years for a conviction?
- Prevention or arrest?
- Behind the "8 ball" ?

Law enforcement – issues (1)

1. The RBN are much more sophisticated and organized than we usually give them credit for and even more worrying is they are probably better financed due to their illegal operations.

- One of our major problems is due to their "highest" level of skills also in COMINT they know what most law enforcement is doing anyway.
- They regularly organize associates to test the defenses of governmental and law enforcement servers and have penetrated many.

Law enforcement – issues (2)

2. The sudden move by the RBN Nov 7th 07 was not due to public disclosure, it is simple to show they planned their deceptive move commencing May 07.

- Perhaps they knew certain law enforcement was getting close.
- More importantly the old RBNetwork and Seychelles connectivity had become more of a liability than an asset.
- Improved fast-flux botnet technology.
- Probable political purposes.

Law enforcement – issues (3)

3. The RBN is monopolistic, as any major criminal or insurgency organization, they do not approve of competition.

- It is well known they see hired "money mules" as disposable
- Perhaps they will also allow or quietly provide information to law enforcement information via third parties; on minor, localized or maverick players which also takes the heat off them.

Law enforcement – issues (4)

4. Should research on BadWare, attack vectors, or investigation of cyber criminal activity itself, remain private to law enforcement to facilitate arrests? If so how?

- No doubt many law enforcement keep such information within "secure" networks, is it 100% safe?
- Does law enforcement have the skills and up to date knowledge
- Co-ordination of different law enforcement bodies an international
- Open source, journalists, EFF and the Internet freedom

Law enforcement – issues (5)

5. The technology the RBN uses, has advanced considerably recently, e.g. the latest ZeuS / Universal code technology allowing for improved fast-flux / double-flux botnet operation.

- There has been very little publicity on the recent increasing size of botnets connected to the Zhelatin (Storm Worm).
- Even information which clearly indicated that the 'Storm' botnet was made up of more than 2 million victim machines was effectively overlooked.
- Note: Zhelatin, Warezov, Bancos aam, Bzub and now Gpcode ai, are all from the same source, and about to become polymorphic.
- The bad news? – With Tor ,Onion router, SSL based FTP, and an off-shore bank account, this could operated from anywhere, even from inside the UK.

Law enforcement – issues (6)

6. The recent blackmailer or ramsomware attacks, with a few very hard to find references, these are continuing.

- Obviously some major corporations (e.g. American Airlines, Booz Allen Hamilton) apparently paid the extortion to avoid any publicity.
- There was some limited interest due to the disclosure by Prevx of martin-golf (dot) net and some said this made the RBN / exploit watchers watch other watchers :)
- But this also shows the reverse problem of no disclosure or pubic awareness at all.

Law enforcement – UK

- SOCA e-crime unit – "Our mission is to prevent harm to UK citizens, but investigations and trials can take three or four years. I think we need to intervene sooner to make things harder for e-criminals."
- "Soca's strategy is to gather intelligence about threats and the methods used, attack them, and so cut the room criminals have to operate,"
- Soca has 4,000 staff and a budget of £416m – but only 150 special constables are trained with the intensive IT skills.
- House of Lords - central e-crime unit - http://petitions.pm.gov.uk/ecrime/

Questions

- Law enforcement, research, the Internet – a synergy?
- Viewing the problem, all the RBN actions are deceitful?
- Common linguistics?
- Can we simplify the inherent complexity?
- Can we match their speed and maybe even be ahead of the game?

Towards solutions and STOP

- **Sociological**
  - Internet community - InfoSEC multi-discipline approach
  - Ethnomethodological approach - Common linguistics
- **Technological**
  - Human centered systems, user-centric controls.
  - Fast-flux, botnet detection,
- **Educational**
  - Educating , interaction, and the research arm of law enforcement
  - Awareness, openness of the internet, assist the media.
- **Radical community action:**
  - Fake the fakes, deceive the deceivers, hack the hackers, spam the spambots?
  - Marine Insurance COMINT approach – Pro-Vigilante; e.g. Layered Tech, botnet

Conclusion

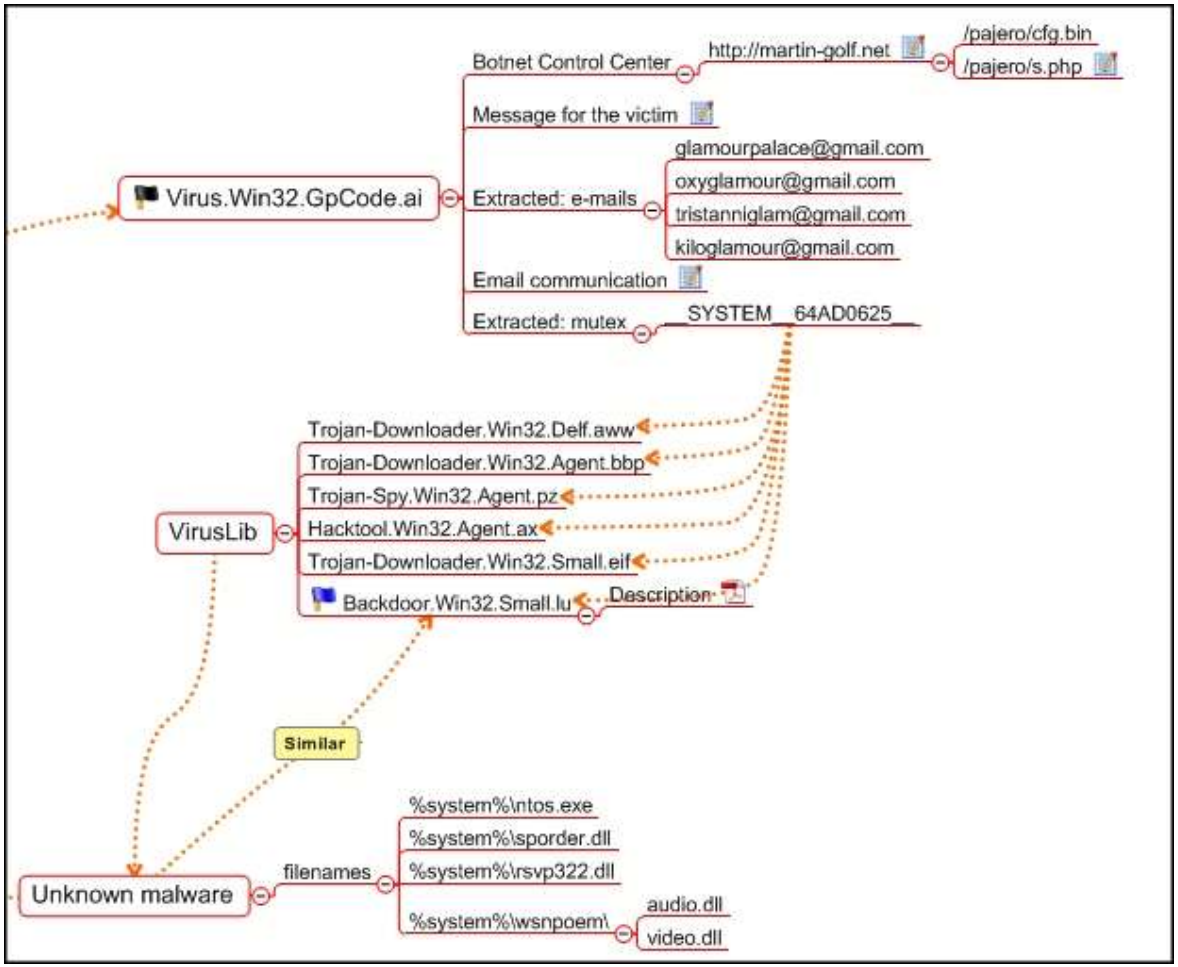
Perhaps the solution lies not in broad, sweeping restrictions (whether from ISPs, regulators, etc.) such as blocking protocols or prohibiting certain types of technical behavior, but rather in providing more user-centric controls that give users more power to protect themselves without restricting access.

Addendum

- Tracking an RBN exploit (3 pages) – viruslist.com – 11/30/07
- User-centric – home control (1 page) – James McQuaid Bleeding Threats - 12/02/07

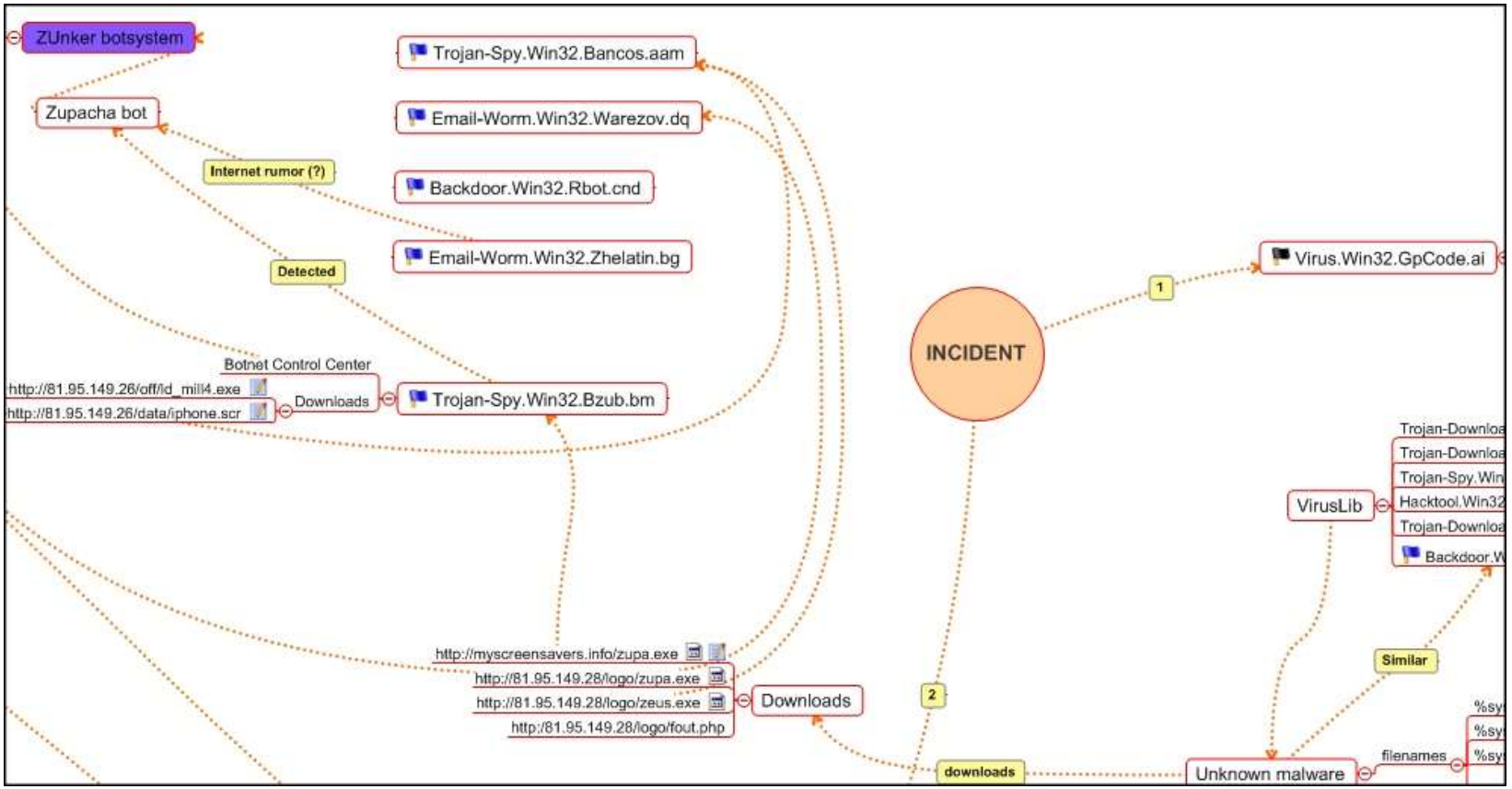
- References:
  - Steve Gibson – Keynote; Anti-Spyware Coalition's annual public workshop Jun 07
  - David Bizeul – RBN Study – 11/21/07
  - Searching for Evil – Prof Ross Anderson & Dr. Richard Clayton – Video talk to Google 08/23/07
  - StopBadWare, Bleeding Threats, Sunbelt, Robtex, CastleCops

Tracking an exploit (ransomware) – (1)



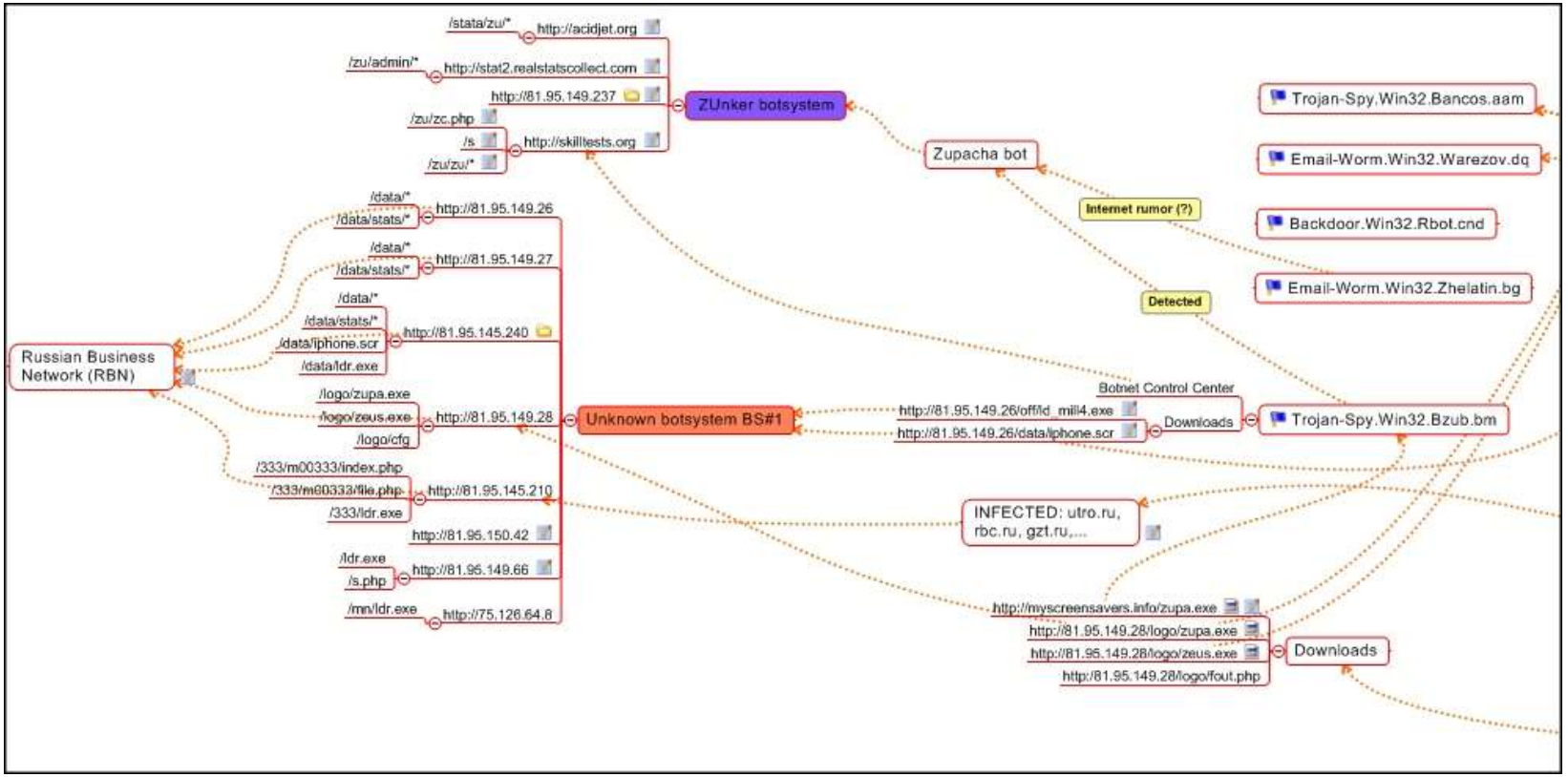
Ref: viruslist.com - 11/30/07

Tracking an exploit (ransomware) – (2)



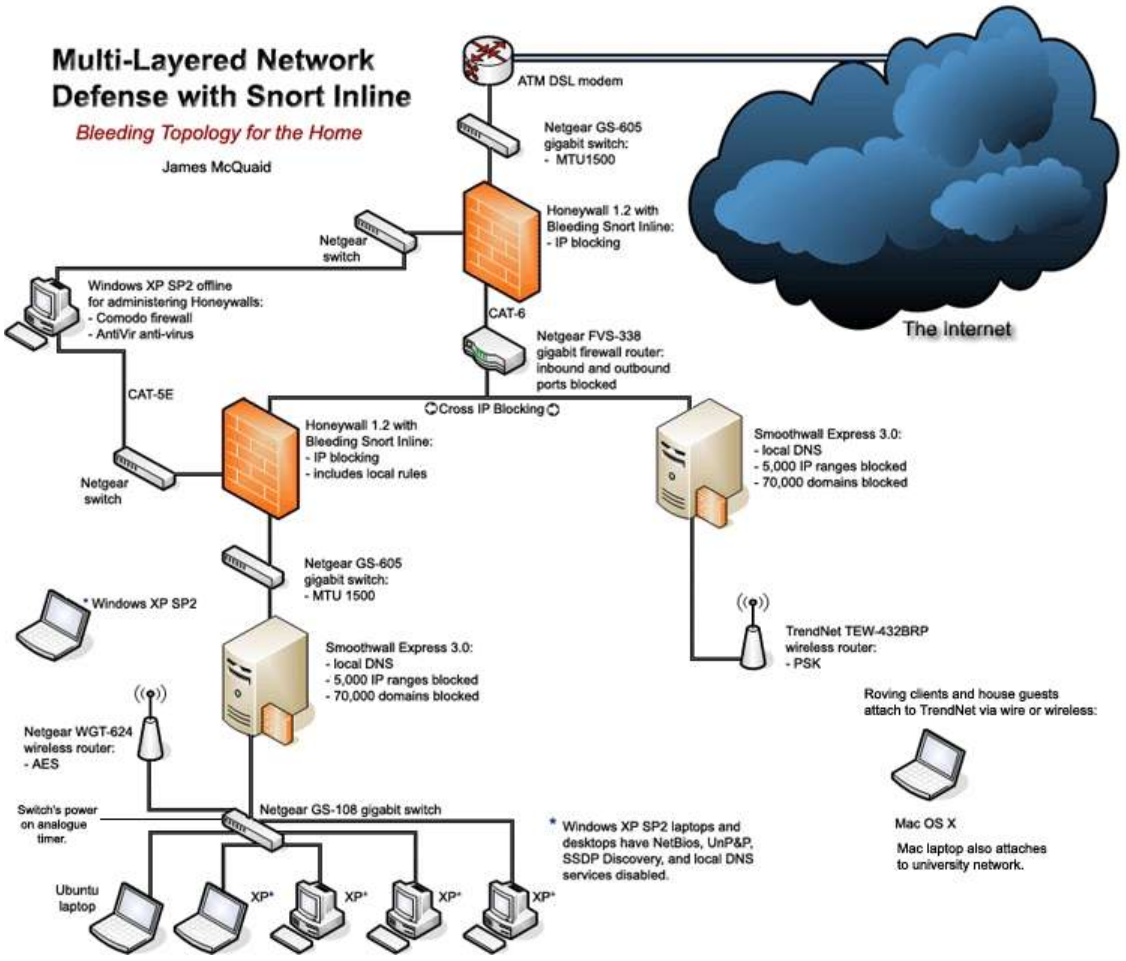
Ref: viruslist.com - 11/30/07

Tracking an exploit (ransomware) – (3)



Ref: viruslist.com - 11/30/07

User-centric – home control



RBNexploit.com

KEEPING AN EYE ON THE RUSSIAN BUSINESS NETWORK

Bad Mal Web

Hide and Seek on the Web

COREXVII

COREXVII.com – Intelligent and focused information