VeriSign®

2007 Trends and 2008 Predictions

Verisign iDefense Security Intelligence Services

Rick Howard - Intelligence Director

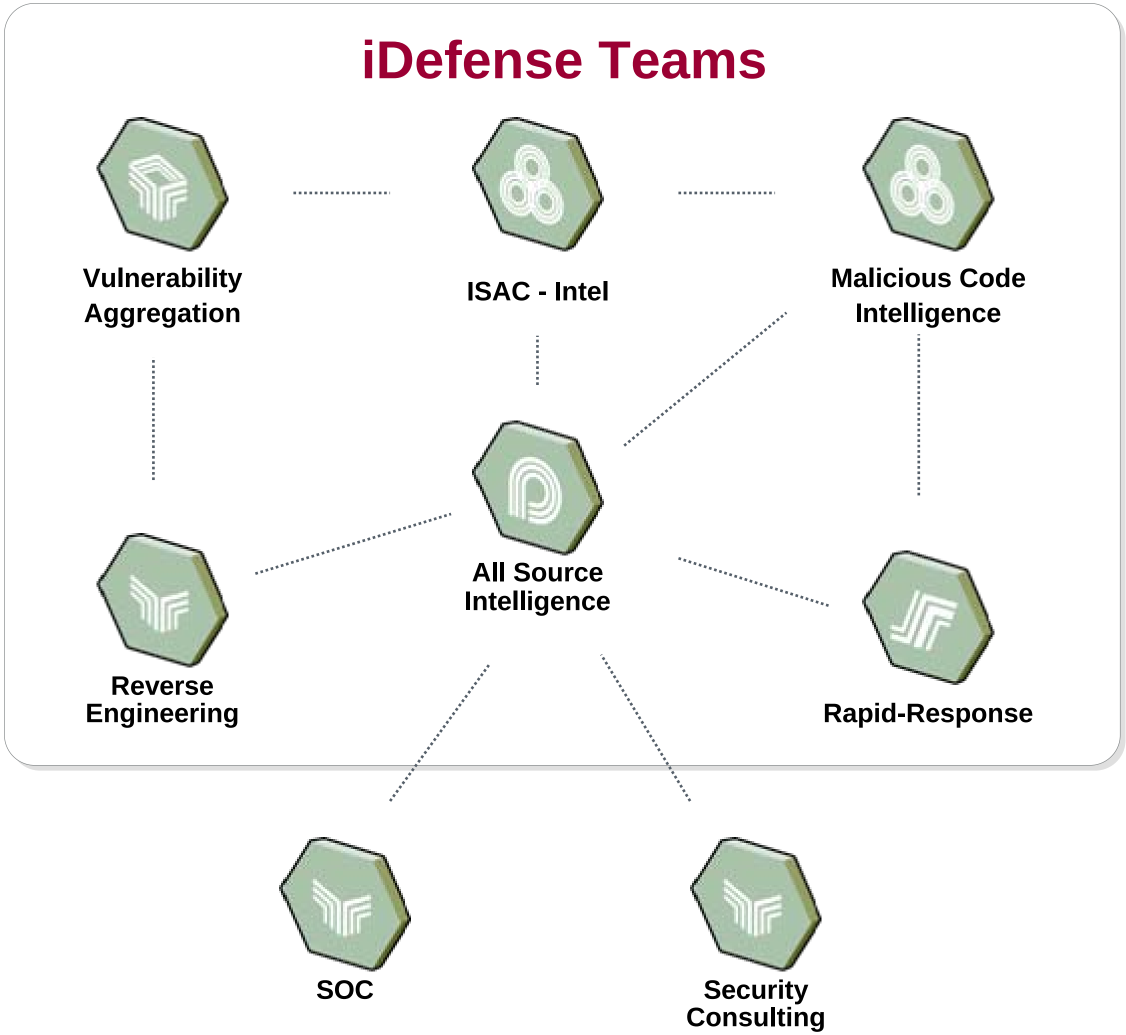
February 2008

Where it all comes together.™

Agenda

General Trends | Motivations | Innovation | Disruptors

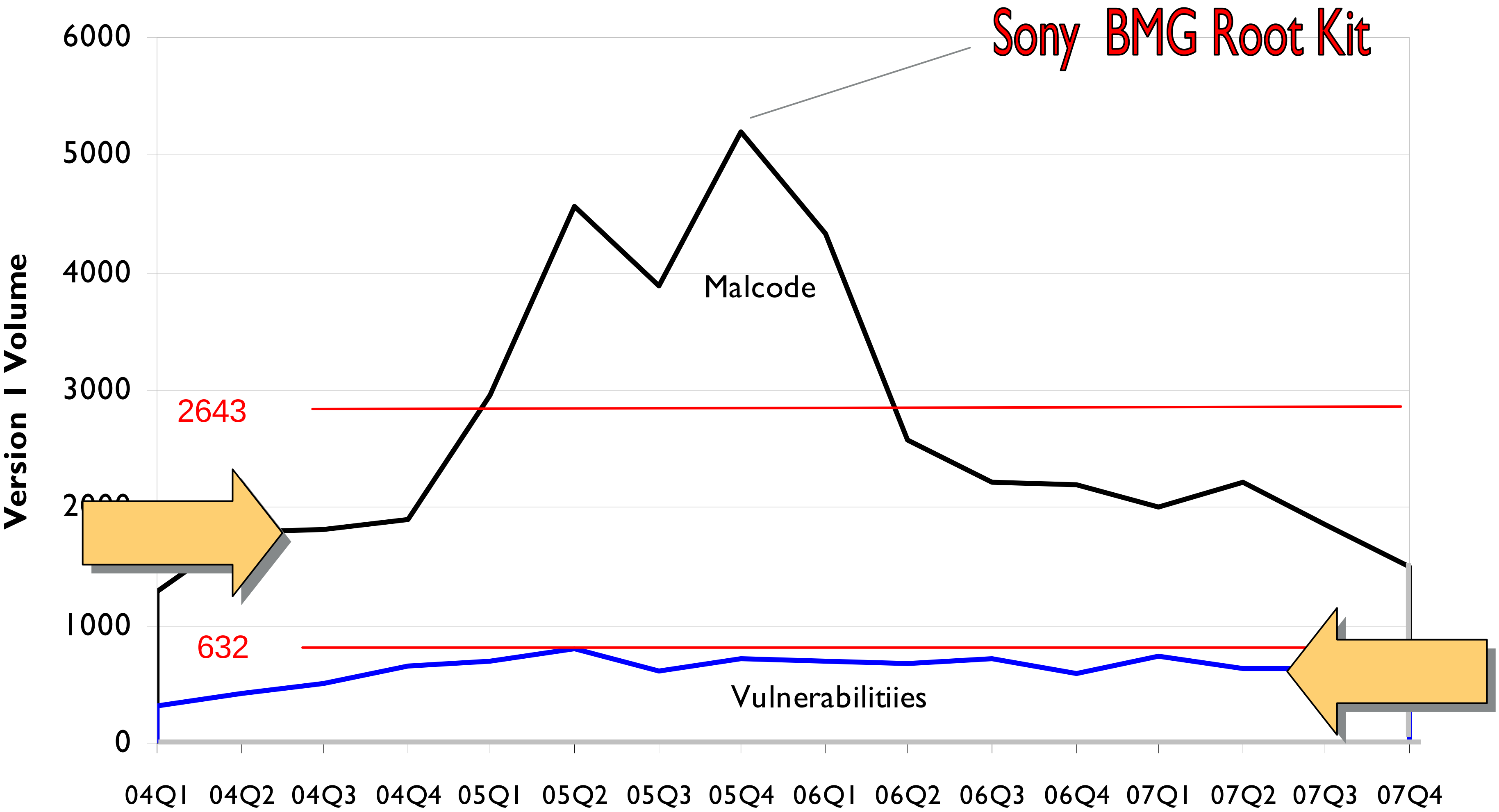
Enterprise Security Group Teams



Agenda

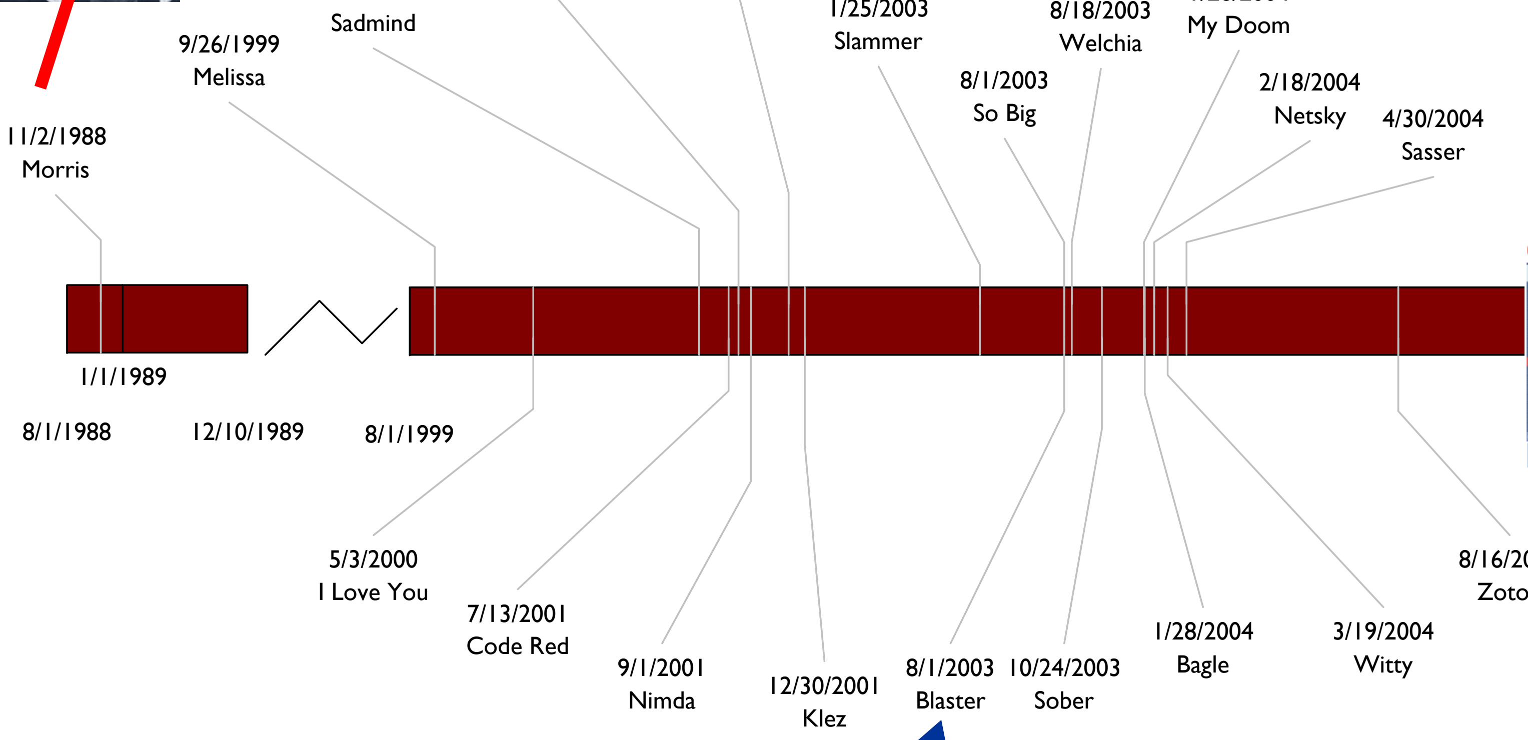
General Trends | Motivations | Innovation | Disruptors

Malcode vs Vulnerabilities Volume



Global Events

www.caida.org



8/1/1988

11/2/1988
Morris

1/1/1989

12/10/1989

8/1/1999

9/26/1999
Melissa

5/3/2000
I Love You

5/8/2001
Sadmind

7/13/2001
Code Red

8/4/2001
Code Red II

9/1/2001
Nimda

11/24/2001
Bad Trans

12/30/2001
Klez

1/25/2003
Slammer

8/1/2003
So Big

8/1/2003
Blaster

8/18/2003
Welchia

10/24/2003
Sober

1/26/2004
My Doom

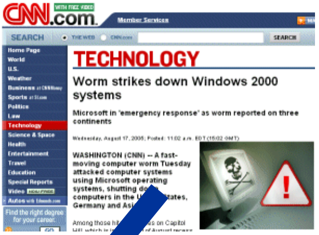
1/28/2004
Bagle

2/18/2004
Netsky

3/19/2004
Witty

4/30/2004
Sasser

8/16/2005
Zotob



CNN.com WITH FREE VIDEO

Member Services

SEARCH ● THE WEB ○ CNN.com SEARCH

Home Page
World
U.S.
Weather
Business at CNNMoney
Sports at SI.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Travel
Education
Special Reports
Video NOW FREE
Autos with Edmunds.com

Find the right degree for your career.

TECHNOLOGY

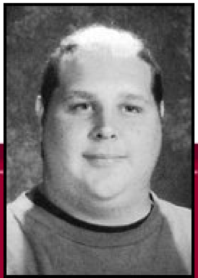
Worm strikes down Windows 2000 systems

Microsoft in 'emergency response' as worm reported on three continents

Wednesday, August 17, 2005; Posted: 11:02 a.m. EDT (15:02 GMT)

WASHINGTON (CNN) -- A fast-moving computer worm Tuesday attacked computer systems using Microsoft operating systems, shutting do computers in the U States, Germany and Asi

Among those hit es on Capitol



Jefferey Lee

Agenda

General Trends Motivations Innovation Disruptors

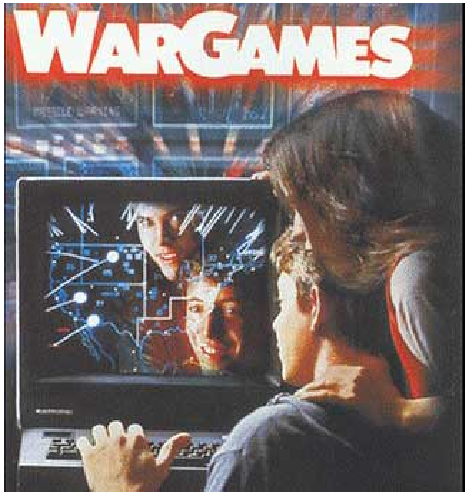
Motivations

- Cyber War
- Espionage
- Religious
- Activists
- Financial

Motivations

- **Cyber War**
- Espionage
- Religious
- Activists
- Financial

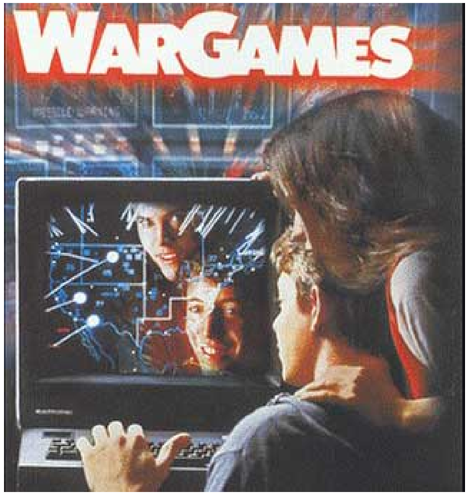
Cyber Riot



Motivations

- **Cyber War**
- Espionage
- Religious
- Activists
- Financial

Proof of Concept



Motivations

- Cyber War
- **Espionage**
- Religious
- Activists
- Financial

Canadian Security Intelligence Service

$1,000,000,000 a month

Motivations

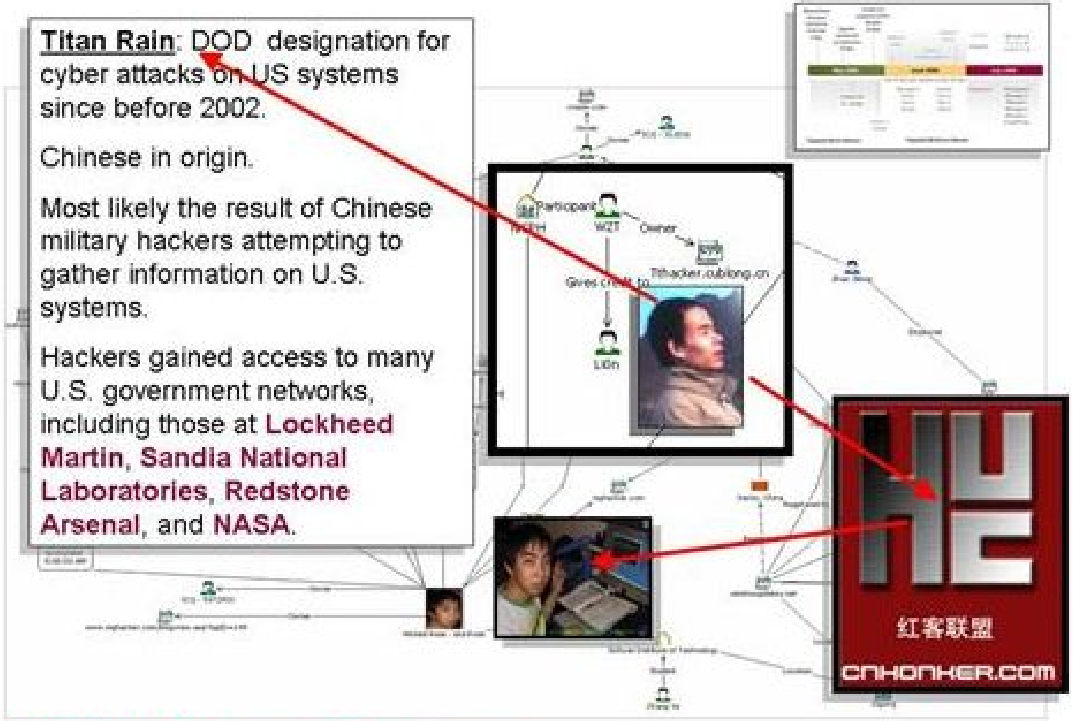
- Cyber War
- **Espionage**
- Religious
- Activists
- Financial

“There is substantial concern, China is stealing our secrets in an effort to leap ahead in terms of its military technology, but also the economic capability of China. It is a substantial threat that we are addressing in the sense of building our program to address this threat.”

-- FBI Director Robert S. Mueller III – Jul 2007

Motivations

- Cyber War
- **Espionage**
- Religious
- Activists
- Financial



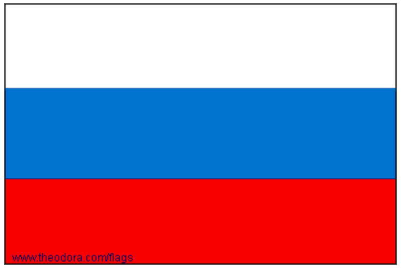
Titan Rain: DOD designation for cyber attacks on US systems since before 2002.

Chinese in origin.

Most likely the result of Chinese military hackers attempting to gather information on U.S. systems.

Hackers gained access to many U.S. government networks, including those at **Lockheed Martin**, **Sandia National Laboratories**, **Redstone Arsenal**, and **NASA**.

NCPH - Chinese Espionage

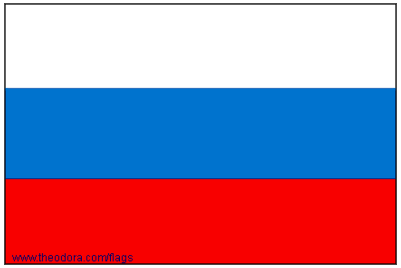


Russian Federation Flag

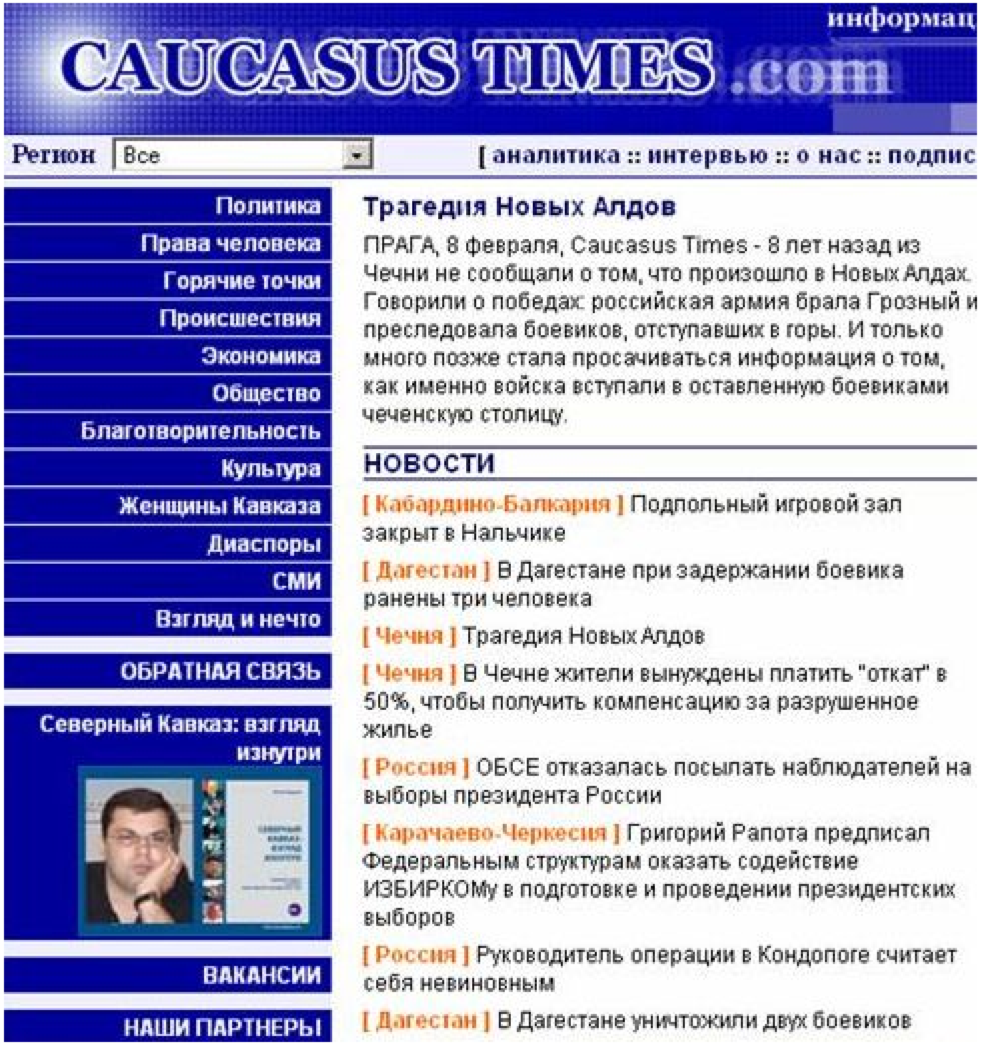
Flags courtesy of www.theodora.com/flags used with permission

Motivations

+ Cyber War
+ **Espionage**
+ Religious
+ Activists
+ Financial



Russian Federation Flag



Трагедия Новых Алдов

ПРАГА, 8 февраля, Caucasus Times - 8 лет назад из Чечни не сообщали о том, что произошло в Новых Алдах. Говорили о победах: российская армия брала Грозный и преследовала боевиков, отступавших в горы. И только много позже стала просачиваться информация о том, как именно войска вступали в оставленную боевиками чеченскую столицу.

НОВОСТИ

[Кабардино-Балкария] Подпольный игровой зал закрыт в Нальчике

[Дагестан] В Дагестане при задержании боевика ранены три человека

[Чечня] Трагедия Новых Алдов

[Чечня] В Чечне жители вынуждены платить "откат" в 50%, чтобы получить компенсацию за разрушенное жилье

[Россия] ОБСЕ отказалась посылать наблюдателей на выборы президента России

[Карачаево-Черкесия] Григорий Рапота предписал Федеральным структурам оказать содействие ИЗБИРКОМу в подготовке и проведении президентских выборов

[Россия] Руководитель операции в Кондопоге считает себя невиновным

[Дагестан] В Дагестане уничтожили двух боевиков

Flags courtesy of www.theodora.com/flags used with permission

Motivations

- Cyber War
- Espionage
- **Religious**
- Activists
- Financial

Propoganda

Militant Islam

Motivations

- Cyber War
- Espionage
- **Religious**
- Activists
- Financial

Recruitment

Militant Islam

Motivations

- Cyber War
- Espionage
- **Religious**
- Activists
- Financial

Financing

Militant Islam

Motivations

- Cyber War
- Espionage
- **Religious**
- Activists
- Financial

Communication

Militant Islam

Motivations

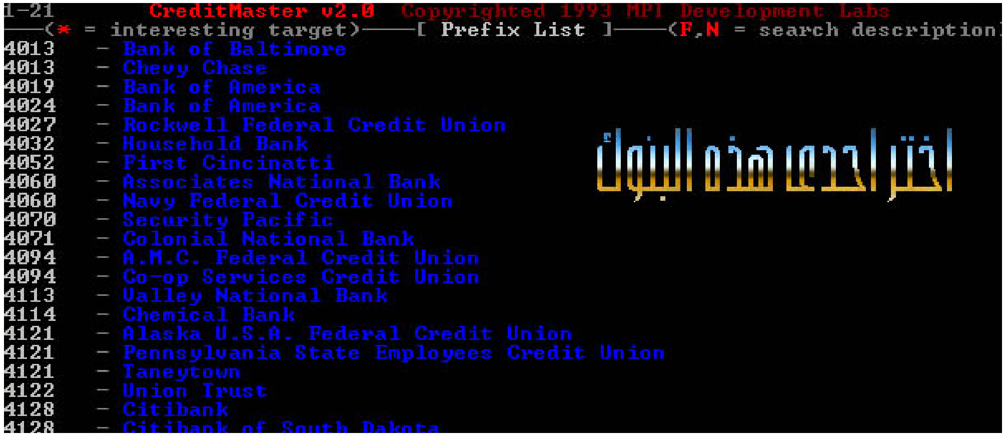
- Cyber War
- Espionage
- **Religious**
- Activists
- Financial

Operational Support

Militant Islam

Motivations

- + Cyber War
- + Espionage
- + **Religious**
- + Activists
- + Financial



```
1-21          CreditMaster v2.0  Copyrighted 1993 MPI Development Labs
───(* = interesting target)────[ Prefix List ]────(F,N = search description
4013    - Bank of Baltimore
4013    - Chevy Chase
4019    - Bank of America
4024    - Bank of America
4027    - Rockwell Federal Credit Union
4032    - Household Bank
4052    - First Cincinatti
4060    - Associates National Bank
4060    - Navy Federal Credit Union
4070    - Security Pacific
4071    - Colonial National Bank
4094    - A.M.C. Federal Credit Union
4094    - Co-op Services Credit Union
4113    - Valley National Bank
4114    - Chemical Bank
4121    - Alaska U.S.A. Federal Credit Union
4121    - Pennsylvania State Employees Credit Union
4121    - Taneytown
4122    - Union Trust
4128    - Citibank
4128    - Citibank of South Dakota
```

E-Jihad v.3.0 (An Arabic tool)

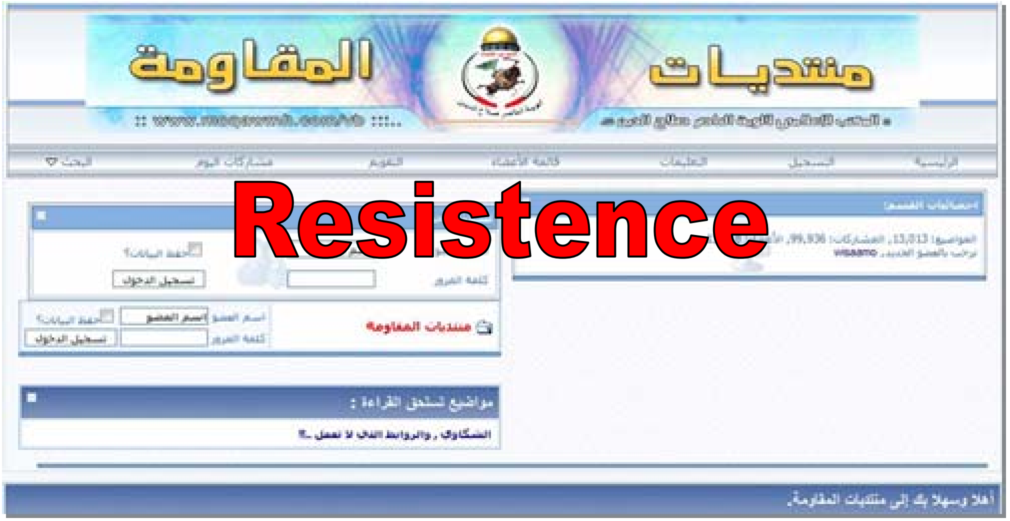
Tsunami v.4.0 (An Arabic tool)

Doraah v.1.5 (An Arabic tool)

Evilping (Converted Western Tool)

Haktek (Converted Western Tool)

Web hakrez (Converted Western Tool)



Motivations

- + Cyber War
- + Espionage
- + **Religious**
- + Activists
- + Financial

E-Jihad v.3.0 (An Arabic tool)

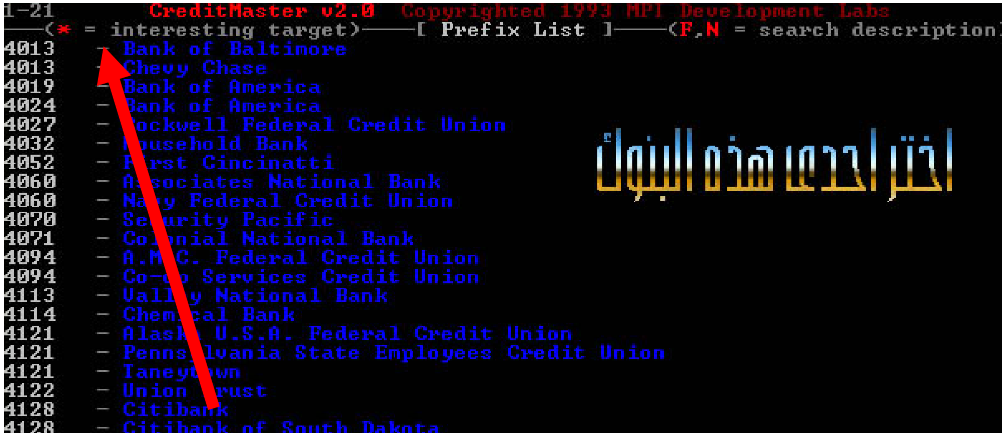
Tsunami v.4.0 (An Arabic tool)

Doraah v.1.5 (An Arabic tool)

Evilping (Converted Western Tool)

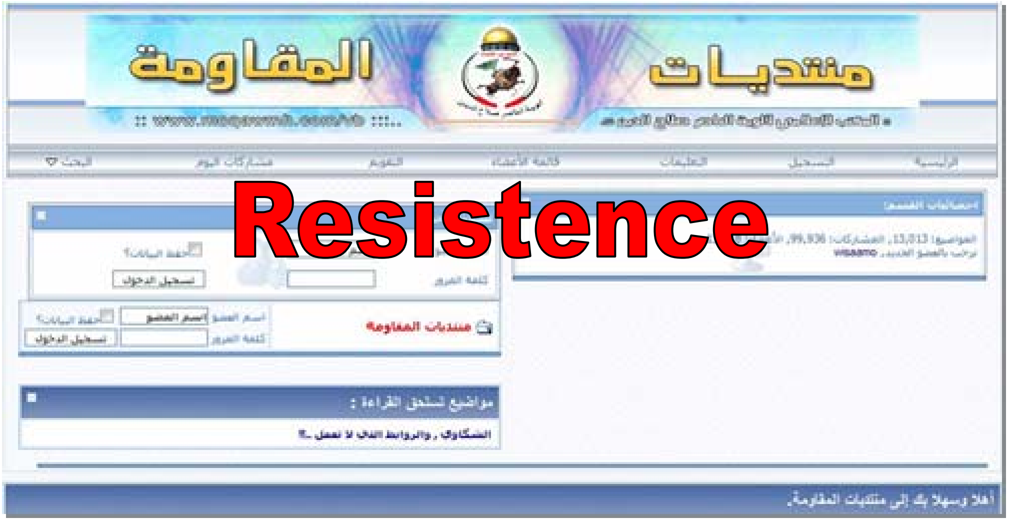
Haktek (Converted Western Tool)

Web hakrez (Converted Western Tool)



```
1-21        CreditMaster v2.0  Copyrighted 1993 MPI Development Labs
───(* = interesting target)────[ Prefix List ]────(F,N = search description)
4013    - Bank of Baltimore
4013    - Chevy Chase
4019    - Bank of America
4024    - Bank of America
4027    - Rockwell Federal Credit Union
4032    - Household Bank
4052    - First Cincinatti
4060    - Associates National Bank
4060    - Navy Federal Credit Union
4070    - Security Pacific
4071    - Colonial National Bank
4094    - A.M.C. Federal Credit Union
4094    - Co-op Services Credit Union
4113    - Valley National Bank
4114    - Chemical Bank
4121    - Alaska U.S.A. Federal Credit Union
4121    - Pennsylvania State Employees Credit Union
4121    - Taneytown
4122    - Union Trust
4128    - Citibank
4128    - Citibank of South Dakota
```

Bank of Baltimore



Resistence

VeriSign

Motivations

- + Cyber War
- + Espionage
- + **Religious**
- + Activists
- + Financial

E-Jihad v.3.0 (An Arabic tool)

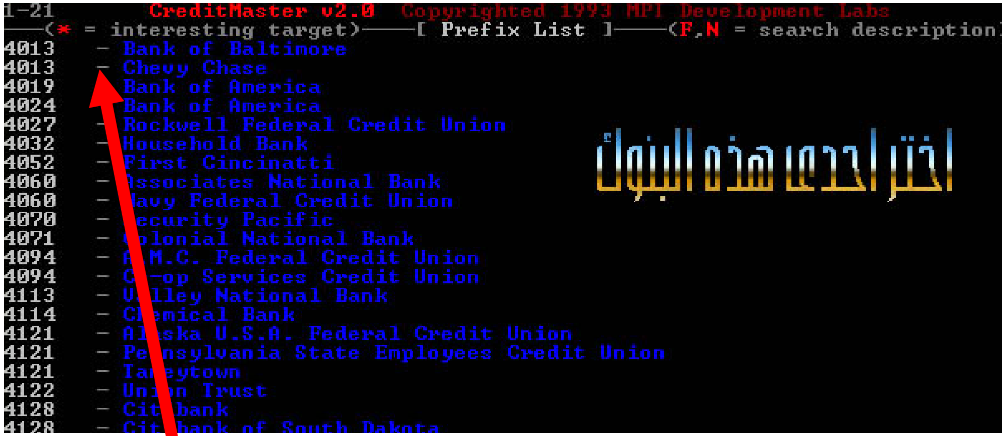
Tsunami v.4.0 (An Arabic tool)

Doraah v.1.5 (An Arabic tool)

Evilping (Converted Western Tool)

Haktek (Converted Western Tool)

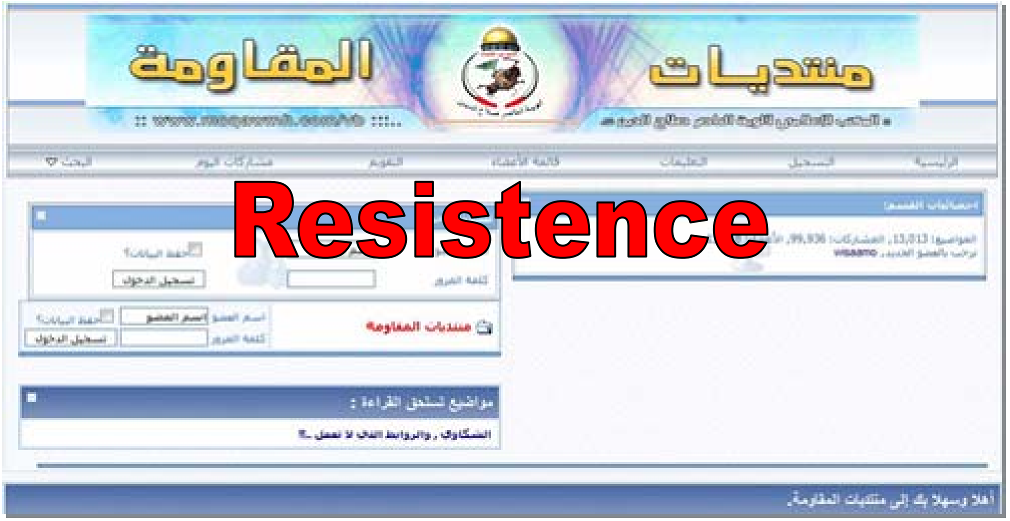
Web hakrez (Converted Western Tool)



```
1-21         CreditMaster v2.0  Copyrighted 1993 MPI Development Labs
───(* = interesting target)────[ Prefix List ]────(F,N = search description)
4013    - Bank of Baltimore
4013    - Chevy Chase
4019    - Bank of America
4024    - Bank of America
4027    - Rockwell Federal Credit Union
4032    - Household Bank
4052    - First Cincinatti
4060    - Associates National Bank
4060    - Navy Federal Credit Union
4070    - Security Pacific
4071    - Colonial National Bank
4094    - A.M.C. Federal Credit Union
4094    - Co-op Services Credit Union
4113    - Valley National Bank
4114    - Chemical Bank
4121    - Alaska U.S.A. Federal Credit Union
4121    - Pennsylvania State Employees Credit Union
4121    - Taneytown
4122    - Union Trust
4128    - Citibank
4128    - Citibank of South Dakota
```

اختر احدى هذه البنوك

Chevy Chase



الشكاوى , والروابط التى لا تعمل ؟..

أهلا وسهلا بك إلى منتديات المقاومة.

Resistence

Motivations

- + Cyber War
- + Espionage
- + **Religious**
- + Activists
- + Financial

E-Jihad v.3.0 (An Arabic tool)

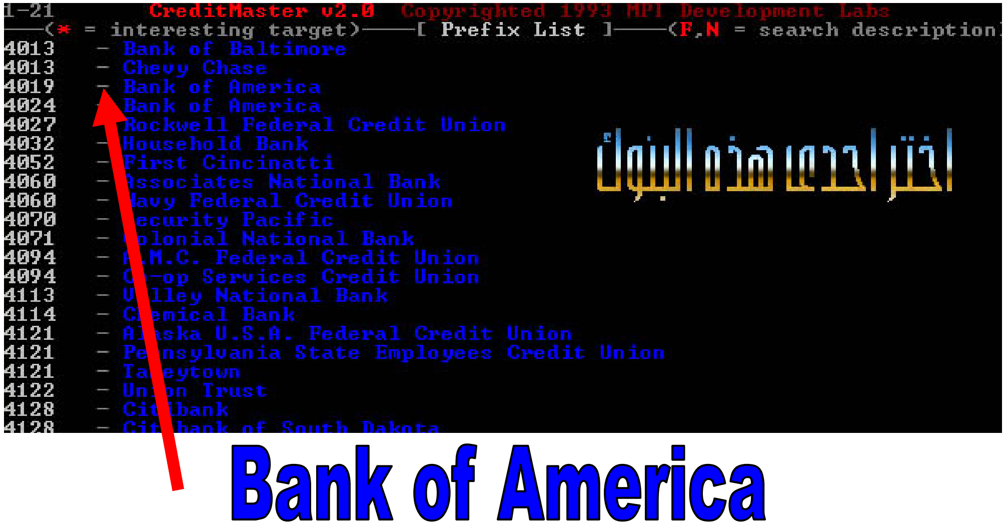
Tsunami v.4.0 (An Arabic tool)

Doraah v.1.5 (An Arabic tool)

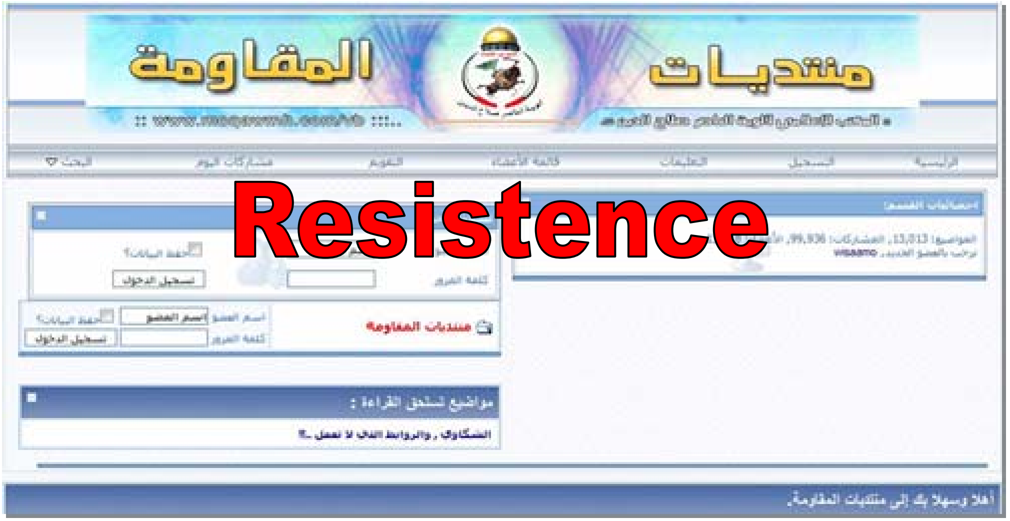
Evilping (Converted Western Tool)

Haktek (Converted Western Tool)

Web hakrez (Converted Western Tool)



```
1-21         CreditMaster v2.0  Copyrighted 1993 MPI Development Labs
───(* = interesting target)────[ Prefix List ]────(F,N = search description
4013    - Bank of Baltimore
4013    - Chevy Chase
4019    - Bank of America
4024    - Bank of America
4027    - Rockwell Federal Credit Union
4032    - Household Bank
4052    - First Cincinatti
4060    - Associates National Bank
4060    - Navy Federal Credit Union
4070    - Security Pacific
4071    - Colonial National Bank
4094    - A.M.C. Federal Credit Union
4094    - Co-op Services Credit Union
4113    - Valley National Bank
4114    - Chemical Bank
4121    - Alaska U.S.A. Federal Credit Union
4121    - Pennsylvania State Employees Credit Union
4121    - Tarreytown
4122    - Union Trust
4128    - Citibank
4128    - Citibank of South Dakota
```



Motivations

- + Cyber War
- + Espionage
- + **Religious**
- + Activists
- + Financial

E-Jihad v.3.0 (An Arabic tool)

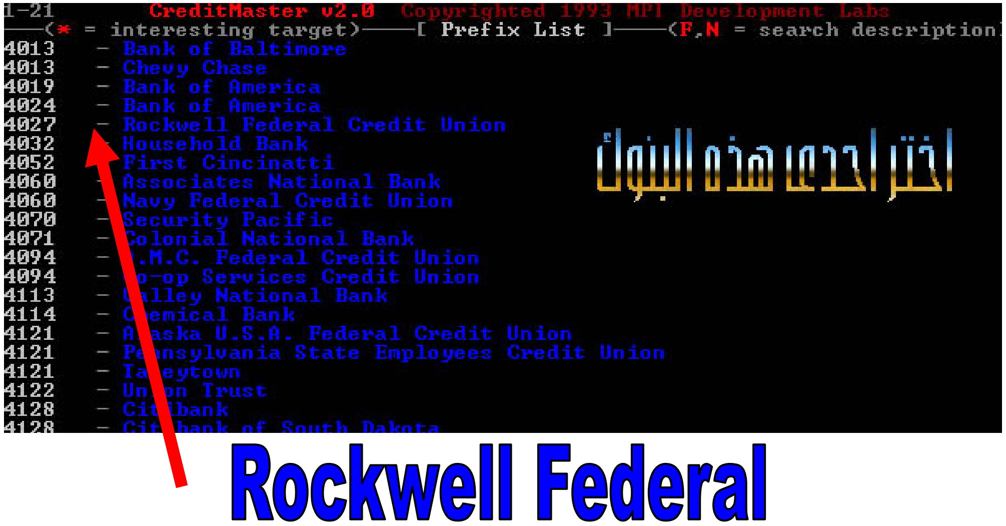
Tsunami v.4.0 (An Arabic tool)

Doraah v.1.5 (An Arabic tool)

Evilping (Converted Western Tool)

Haktek (Converted Western Tool)

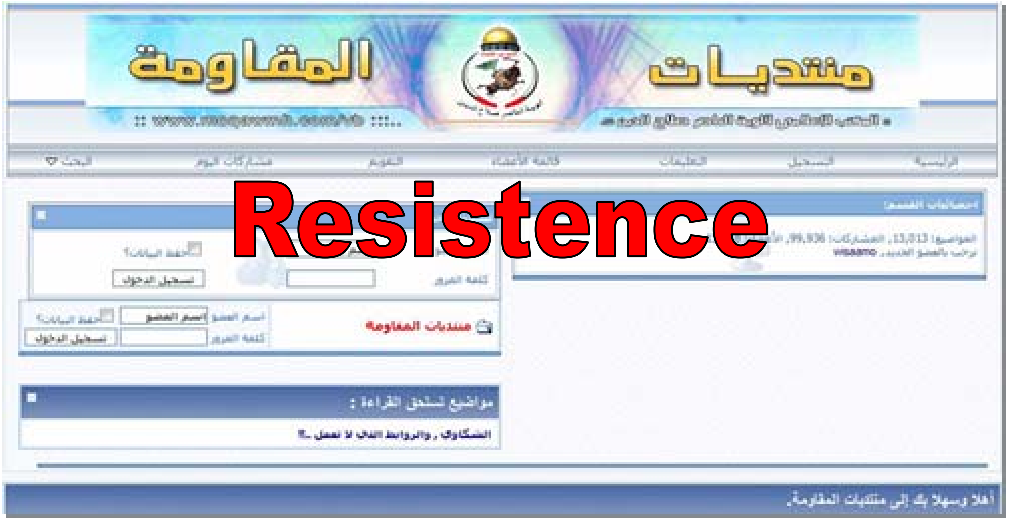
Web hakrez (Converted Western Tool)



```
1-21          CreditMaster v2.0  Copyrighted 1993 MPI Development Labs
───(* = interesting target)───[ Prefix List ]───(F,N = search description
4013    - Bank of Baltimore
4013    - Chevy Chase
4019    - Bank of America
4024    - Bank of America
4027    - Rockwell Federal Credit Union
4032    - Household Bank
4052    - First Cincinatti
4060    - Associates National Bank
4060    - Navy Federal Credit Union
4070    - Security Pacific
4071    - Colonial National Bank
4094    - .M.C. Federal Credit Union
4094    - o-op Services Credit Union
4113    - alley National Bank
4114    - emical Bank
4121    - A aska U.S.A. Federal Credit Union
4121    - Pe nsylvania State Employees Credit Union
4121    - Ta eytown
4122    - Un on Trust
4128    - Cit bank
4128    - Cit bank of South Dakota
```

اختر احدى هذه البنوك

Rockwell Federal



احصائيات القسم

المواضيع: 13,013، المشاركات: 99,936،
ترحب بالعضو الجديد، visaamo

منتديات المقاومة

مواضيع تستحق القراءة :

الشكاوى , والروابط التي لا تعمل ..!!

أهلا وسهلا بك إلى منتديات المقاومة.

Resistence

Motivations

- + Cyber War
- + Espionage
- + **Religious**
- + Activists
- + Financial

E-Jihad v.3.0 (An Arabic tool)

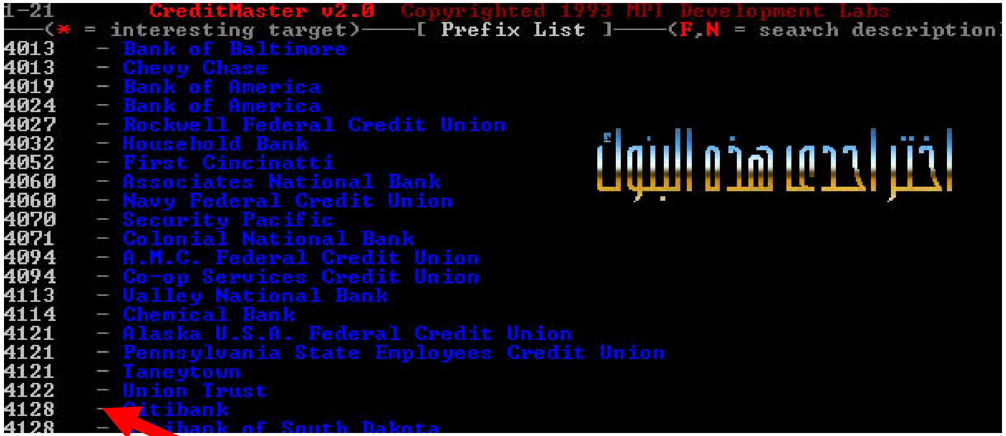
Tsunami v.4.0 (An Arabic tool)

Doraah v.1.5 (An Arabic tool)

Evilping (Converted Western Tool)

Haktek (Converted Western Tool)

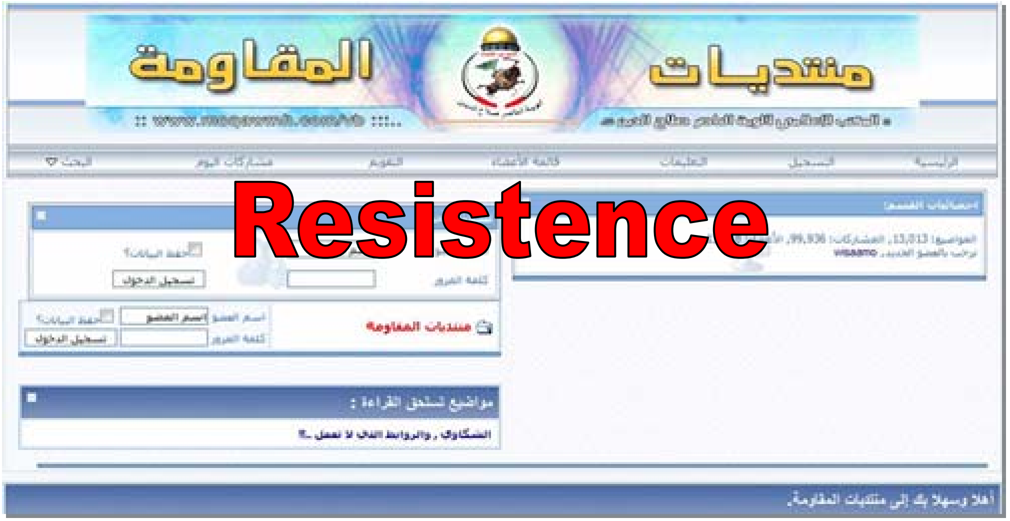
Web hakrez (Converted Western Tool)



```
1-21         CreditMaster v2.0  Copyrighted 1993 MPI Development Labs
───(* = interesting target)───[ Prefix List ]───(F,N = search description)
4013    - Bank of Baltimore
4013    - Chevy Chase
4019    - Bank of America
4024    - Bank of America
4027    - Rockwell Federal Credit Union
4032    - Household Bank
4052    - First Cincinatti
4060    - Associates National Bank
4060    - Navy Federal Credit Union
4070    - Security Pacific
4071    - Colonial National Bank
4094    - A.M.C. Federal Credit Union
4094    - Co-op Services Credit Union
4113    - Valley National Bank
4114    - Chemical Bank
4121    - Alaska U.S.A. Federal Credit Union
4121    - Pennsylvania State Employees Credit Union
4121    - Taneytown
4122    - Union Trust
4128    - Citibank
4128    - Citibank of South Dakota
```

اختر احدى هذه البنوك

CitiBank



مواضيع تستحق القراءة :

الشكاوى , والروابط التي لا تعمل ..؟

أهلا وسهلا بك إلى منتديات المقاومة.

Resistence

Motivations

- Cyber War
- Espionage
- Religious
- **Activists**
- Financial

Controversial Change

Motivations

- Cyber War
- Espionage
- Religious
- **Activists**
- Financial

Environmental and **Animal Rights**

Political activists are members of various political parties, anti-war groups, anarchists, racial & gender-based special interests from equal rights groups to supremacy and hate groups

Religious groups include pro-life and pro-choice supporters

Anti-globalization groups that target the WTO, World Bank, APEC and G8 Meetings

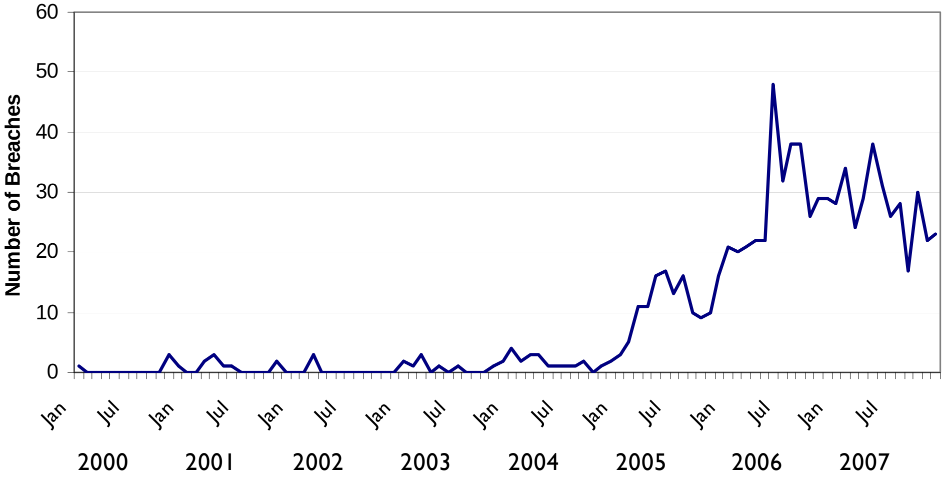
Cyber activism

Do you want to help save the planet?

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Source: Attrition.org – Data Breaches



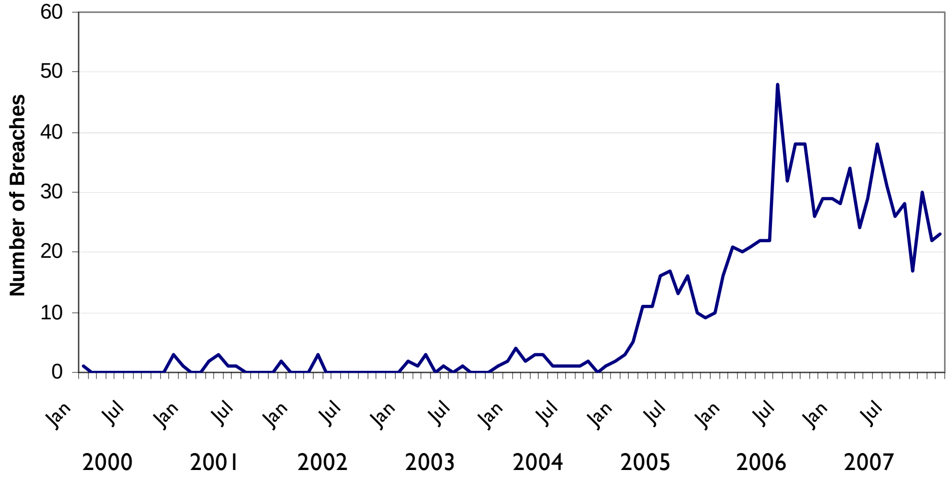
http://etiolated.org/

Cyber Crime: No Longer a Startup

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Source: Attrition.org – Data Breaches



http://etiolated.org/

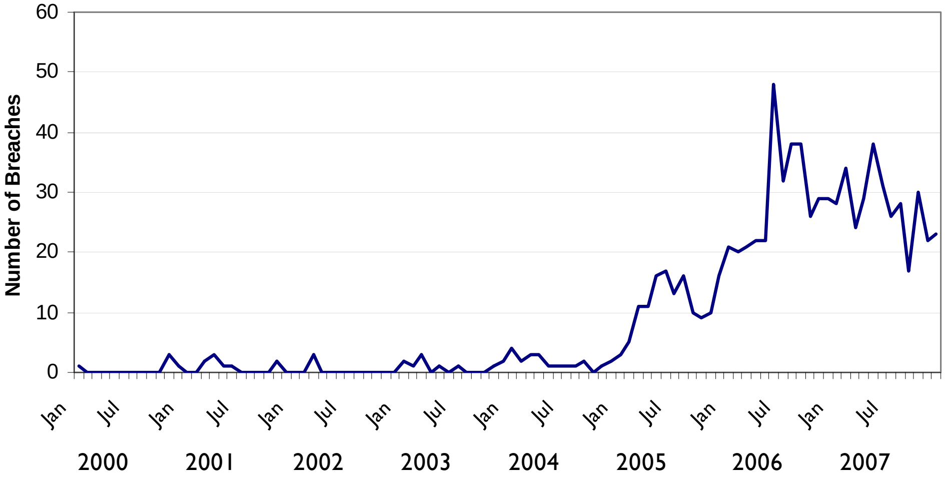
Cyber Crime: No Longer a Startup

HangUp Team

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Source: Attrition.org – Data Breaches



http://etiolated.org/

Cyber Crime: No Longer a Startup

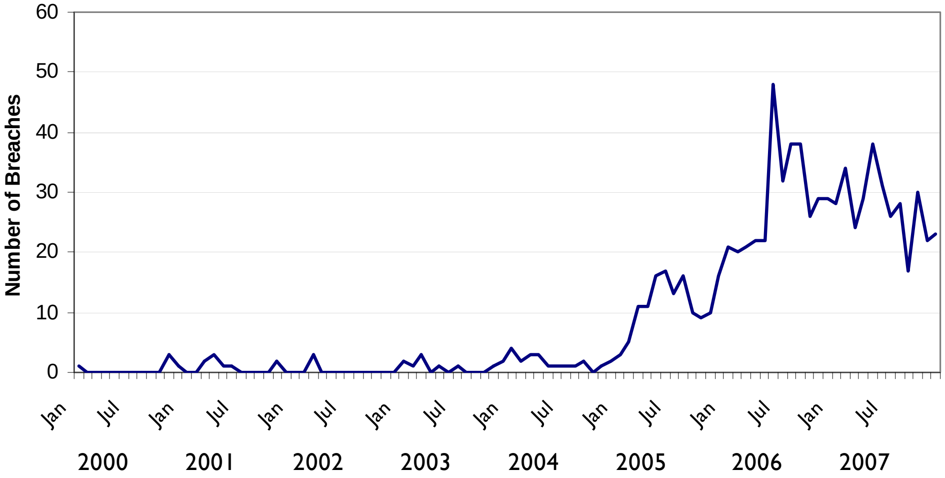
UpLevel

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Cyber Crime: No Longer a Startup

Source: Attrition.org – Data Breaches



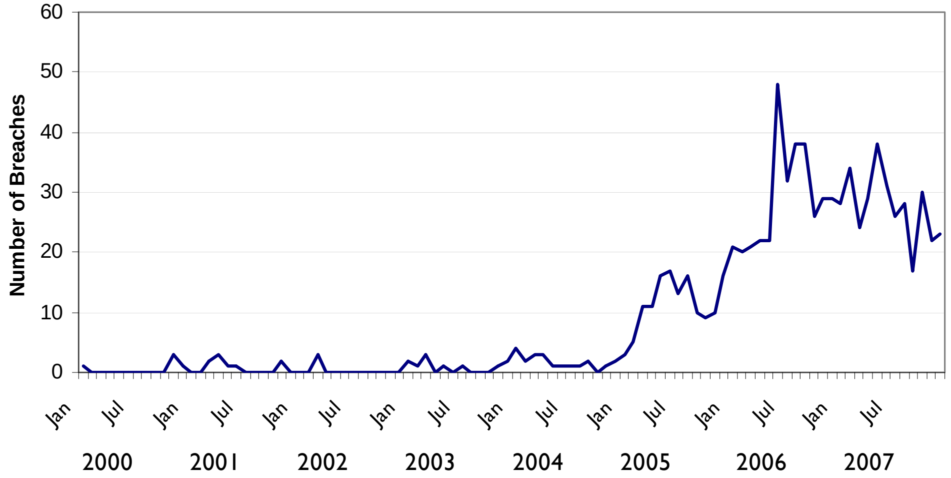
http://etiolated.org/

SASS

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Source: Attrition.org – Data Breaches



http://etiolated.org/

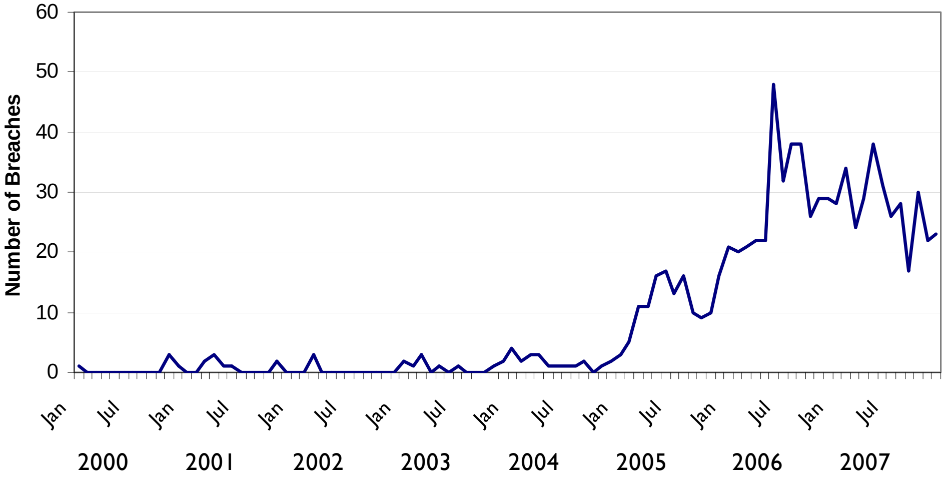
Cyber Crime: No Longer a Startup

The Olate Suite

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Source: Attrition.org – Data Breaches



Cyber Crime: No Longer a Startup

http://etiolated.org/

HangUp Team

UpLevel

SASS

The Olate Suite

Motivations

- Cyber War
- Espionage
- Religious
- Activists
- **Financial**

Cyber Crime: No Longer a Startup

Professionalized

Software QA

Product Enhancement

Customer Tiering Strategies

Marketing and Sales

Business Specialization

HangUp Team

UpLevel

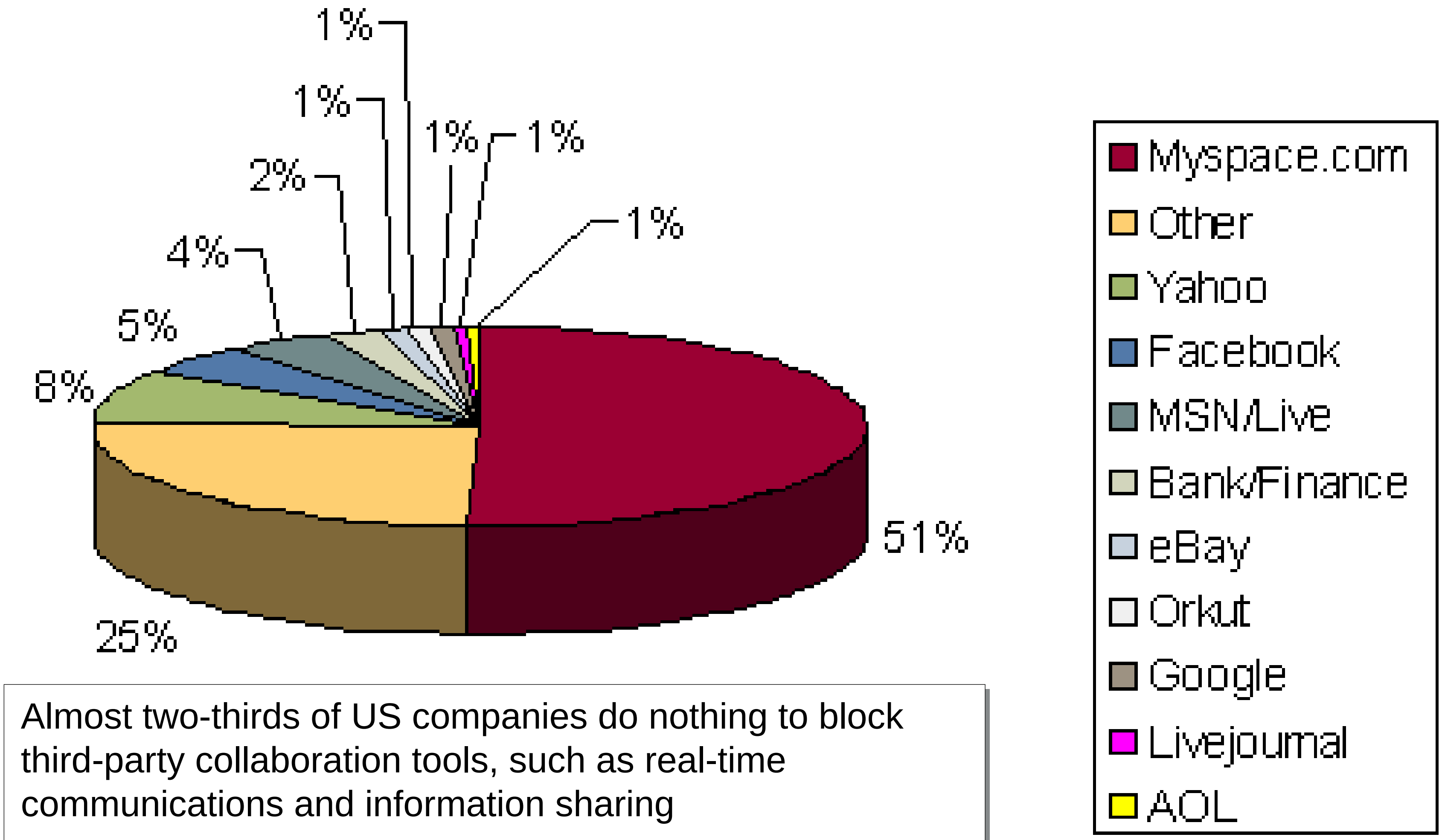
SASS

The Olate Suite

Agenda

General Trends Motivations Innovation Disruptors

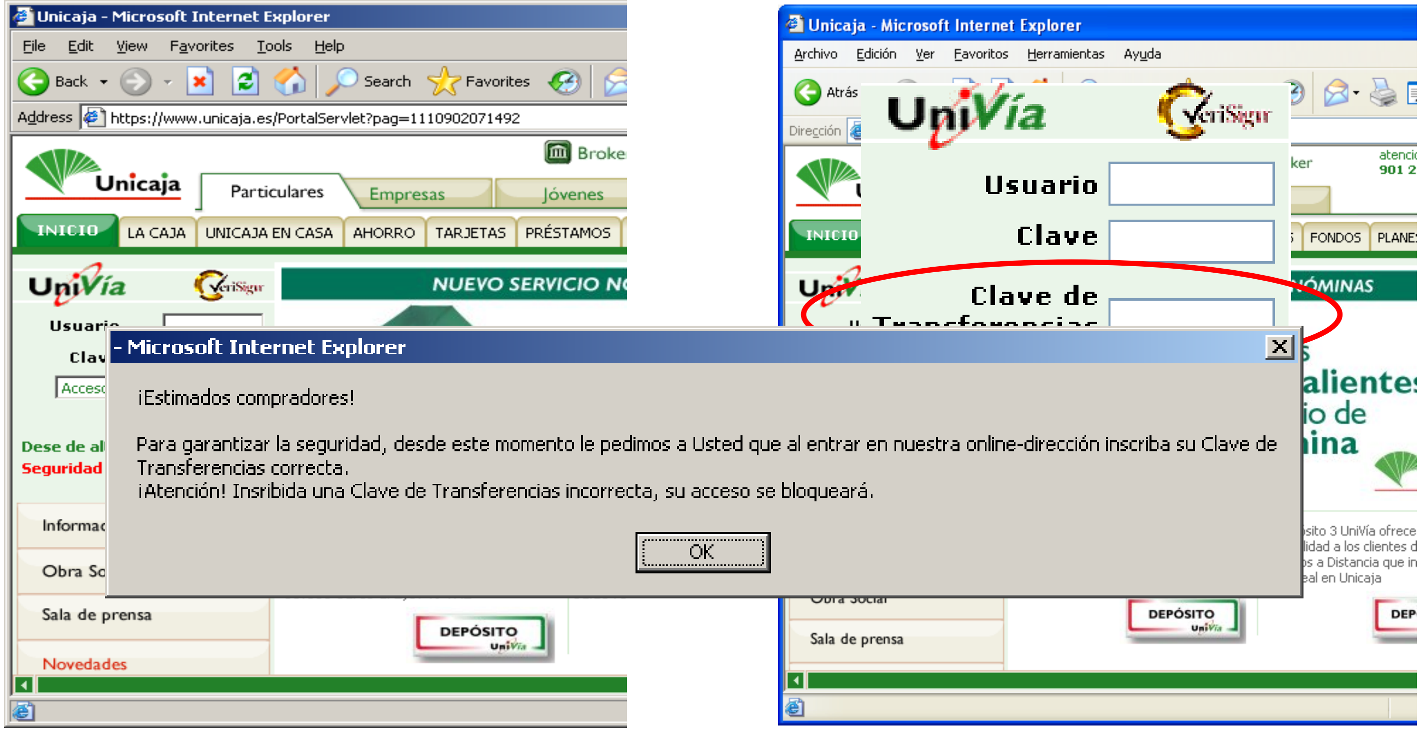
Credential Data Mining



Almost two-thirds of US companies do nothing to block third-party collaboration tools, such as real-time communications and information sharing

Yankee Group – 31 Jan 2008

Metafisher: HTML Injection



Unicaja - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Unicaja
Particulares Empresas Jóvenes
INICIO LA CAJA UNICAJA EN CASA AHORRO TARJETAS PRÉSTAMOS
UniVía
NUEVO SERVICIO N
Novedades
Sala de prensa
DEPÓSITO UniVía
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás
Dirección
INICIO FONDOS PLANE
ÓMINAS
DEPÓSITO UniVía

https://www.unicaja.es/PortalServlet?pag=1110902071492

UniVía

Usuario

Clave

Clave de Transferencias

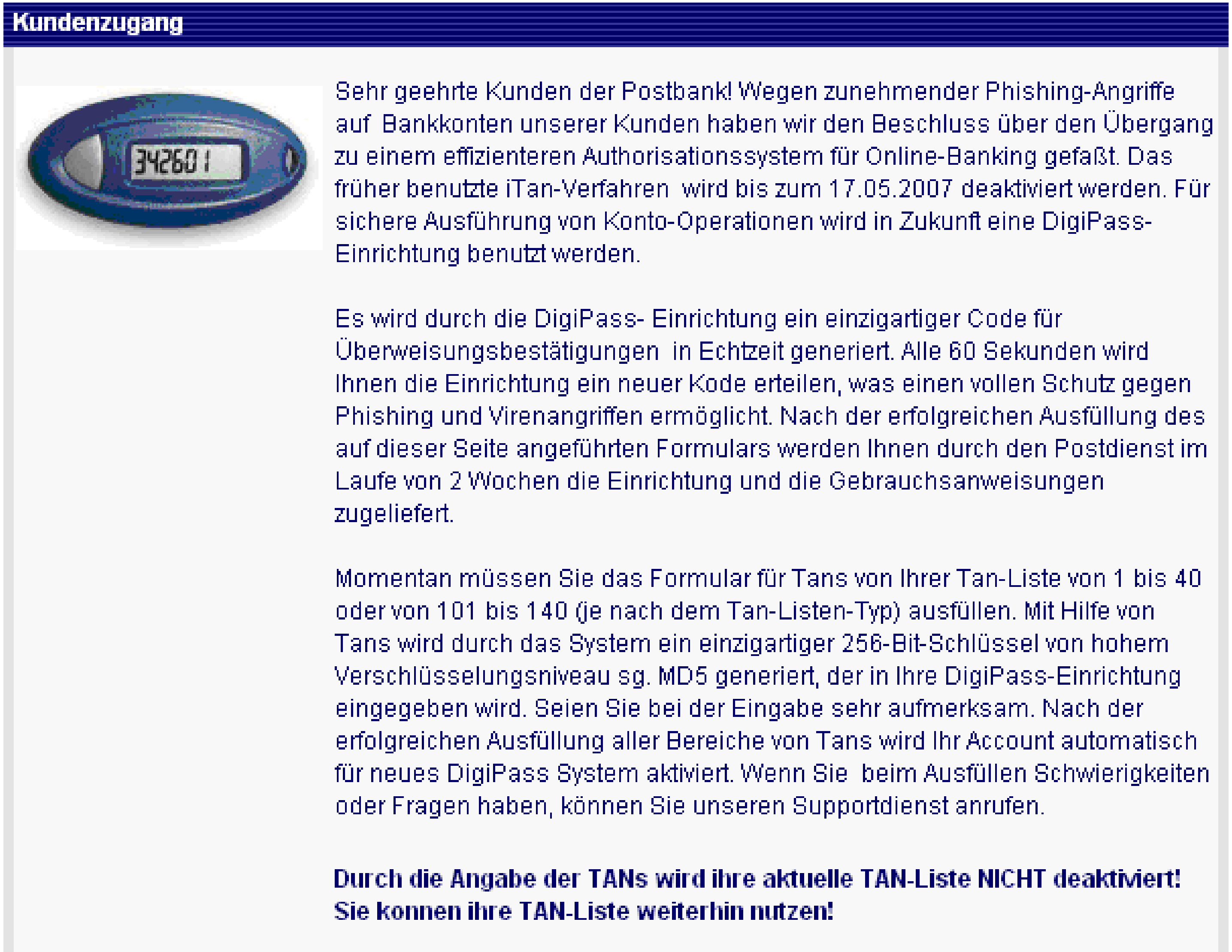
- Microsoft Internet Explorer

¡Estimados compradores!

Para garantizar la seguridad, desde este momento le pedimos a Usted que al entrar en nuestra online-dirección inscriba su Clave de Transferencias correcta.
¡Atención! Insribida una Clave de Transferencias incorrecta, su acceso se bloqueará.

OK

Phishing the second factor



Kundenzugang

Sehr geehrte Kunden der Postbank! Wegen zunehmender Phishing-Angriffe auf Bankkonten unserer Kunden haben wir den Beschluss über den Übergang zu einem effizienteren Authorisationssystem für Online-Banking gefaßt. Das früher benutzte iTan-Verfahren wird bis zum 17.05.2007 deaktiviert werden. Für sichere Ausführung von Konto-Operationen wird in Zukunft eine DigiPass-Einrichtung benutzt werden.

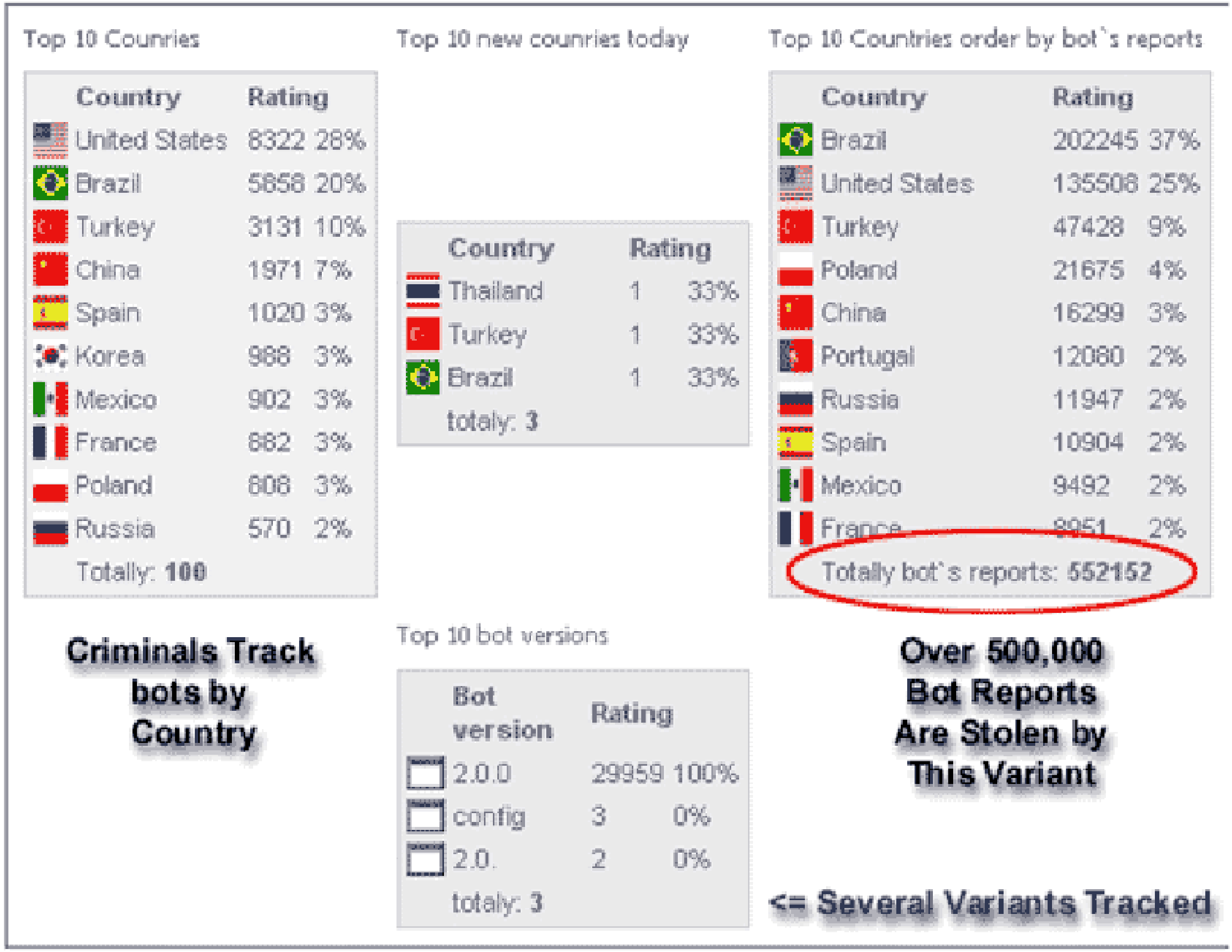
Es wird durch die DigiPass- Einrichtung ein einzigartiger Code für Überweisungsbestätigungen in Echtzeit generiert. Alle 60 Sekunden wird Ihnen die Einrichtung ein neuer Kode erteilen, was einen vollen Schutz gegen Phishing und Virenangriffen ermöglicht. Nach der erfolgreichen Ausfüllung des auf dieser Seite angeführten Formulars werden Ihnen durch den Postdienst im Laufe von 2 Wochen die Einrichtung und die Gebrauchsanweisungen zugeliefert.

Momentan müssen Sie das Formular für Tans von Ihrer Tan-Liste von 1 bis 40 oder von 101 bis 140 (je nach dem Tan-Listen-Typ) ausfüllen. Mit Hilfe von Tans wird durch das System ein einzigartiger 256-Bit-Schlüssel von hohem Verschlüsselungsniveau sg. MD5 generiert, der in Ihre DigiPass-Einrichtung eingegeben wird. Seien Sie bei der Eingabe sehr aufmerksam. Nach der erfolgreichen Ausfüllung aller Bereiche von Tans wird Ihr Account automatisch für neues DigiPass System aktiviert. Wenn Sie beim Ausfüllen Schwierigkeiten oder Fragen haben, können Sie unseren Supportdienst anrufen.

Durch die Angabe der TANs wird ihre aktuelle TAN-Liste NICHT deaktiviert! Sie konnen ihre TAN-Liste weiterhin nutzen!

Underground Customer Service

MetaFisher Command & Control Center



Top 10 Counries

Country	Rating	
United States	8322	28%
Brazil	5858	20%
Turkey	3131	10%
China	1971	7%
Spain	1020	3%
Korea	988	3%
Mexico	902	3%
France	882	3%
Poland	808	3%
Russia	570	2%
Totally: **100**		

Top 10 new counries today

Country	Rating	
Thailand	1	33%
Turkey	1	33%
Brazil	1	33%
totaly: **3**		

Top 10 Countries order by bot`s reports

Country	Rating	
Brazil	202245	37%
United States	135508	25%
Turkey	47428	9%
Poland	21675	4%
China	16299	3%
Portugal	12080	2%
Russia	11947	2%
Spain	10904	2%
Mexico	9492	2%
France	8951	2%
Totally bot`s reports: **552152**		

Criminals Track bots by Country

Top 10 bot versions

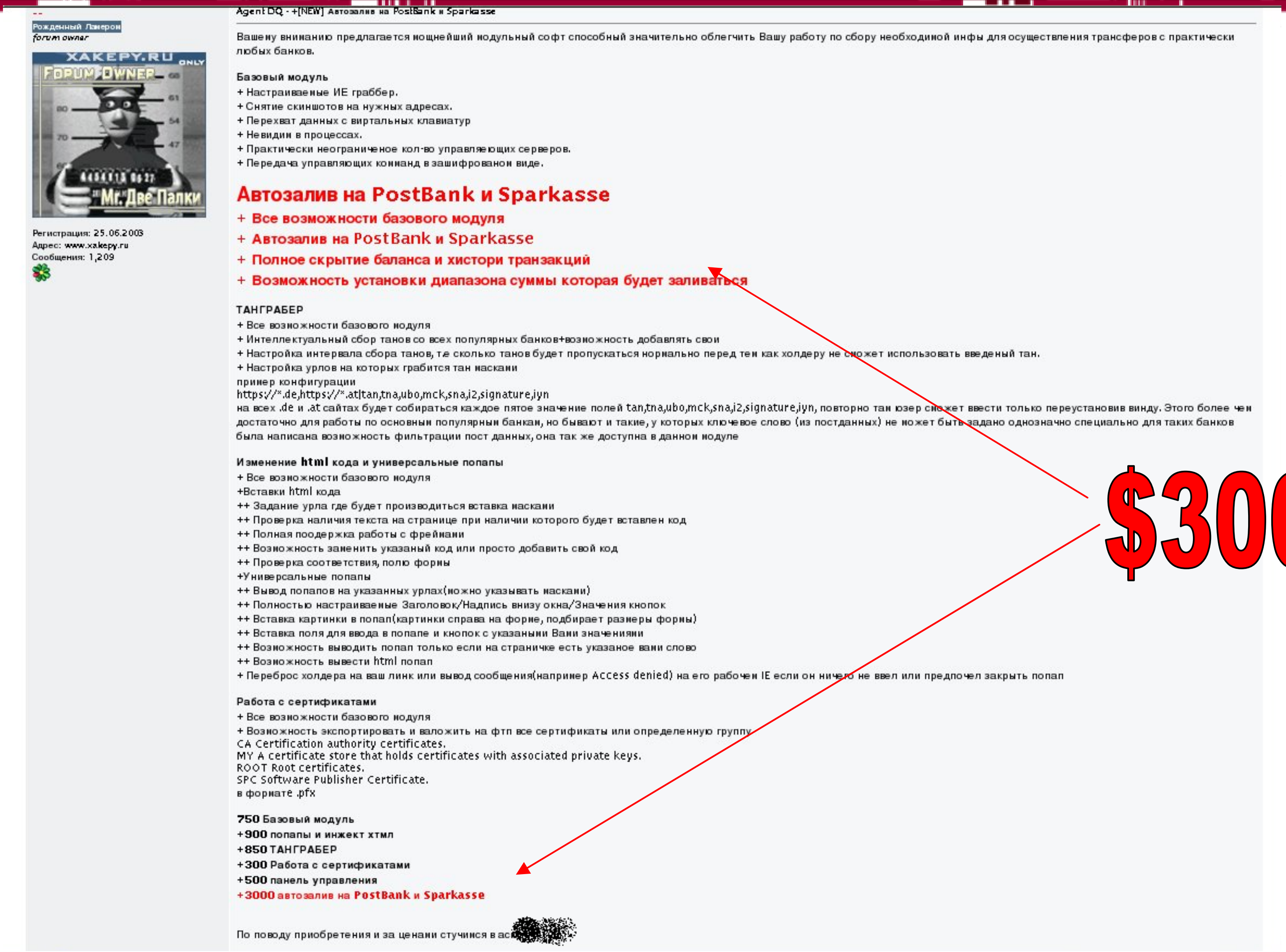
Bot version	Rating	
2.0.0	29959	100%
config	3	0%
2.0.	2	0%
totaly: **3**		

Over 500,000 Bot Reports Are Stolen by This Variant

<= Several Variants Tracked

552,152 Hosts

Add-On Services



--
Рожденный Ламером
forum owner

Регистрация: 25.06.2003
Адрес: www.xakepy.ru
Сообщения: 1,209

Agent DQ - +[NEW] **Автозалив на PostBank и Sparkasse**

Вашему вниманию предлагается мощнейший модульный софт способный значительно облегчить Вашу работу по сбору необходимой инфы для осуществления трансферов с практически любых банков.

Базовый модуль
+ Настраиваемые ИЕ граббер.
+ Снятие скиншотов на нужных адресах.
+ Перехват данных с виртальных клавиатур
+ Невидим в процессах.
+ Практически неограниченое кол-во управляющих серверов.
+ Передача управляющих комманд в зашифрованом виде.

Автозалив на PostBank и Sparkasse

+ Все возможности базового модуля
+ Автозалив на PostBank и Sparkasse
+ Полное скрытие баланса и хистори транзакций
+ Возможность установки диапазона суммы которая будет заливаться

ТАНГРАБЕР
+ Все возможности базового модуля
+ Интеллектуальный сбор танов со всех популярных банков+возможность добавлять свои
+ Настройка интервала сбора танов, т.е сколько танов будет пропускаться нормально перед тем как холдеру не сможет использовать введеный тан.
+ Настройка урлов на которых грабится тан масками
пример конфигурации
https://*.de,https://*.at|tan,tna,ubo,mck,sna,i2,signature,iyn
на всех .de и .at сайтах будет собираться каждое пятое значение полей tan,tna,ubo,mck,sna,i2,signature,iyn, повторно там юзер сможет ввести только переустановив винду. Этого более чем достаточно для работы по основным популярным банкам, но бывают и такие, у которых ключевое слово (из постданных) не может быть задано однозначно специально для таких банков была написана возможность фильтрации пост данных, она так же доступна в данном модуле

Изменение html кода и универсальные попапы
+ Все возможности базового модуля
+Вставки html кода
++ Задание урла где будет производиться вставка масками
++ Проверка наличия текста на странице при наличии которого будет вставлен код
++ Полная поодержка работы с фреймами
++ Возможность заменить указаный код или просто добавить свой код
++ Проверка соответствия, полю формы
+Универсальные попапы
++ Вывод попапов на указанных урлах(можно указывать масками)
++ Полностью настраиваемые Заголовок/Надпись внизу окна/Значения кнопок
++ Вставка картинки в попап(картинки справа на форме, подбирает размеры формы)
++ Вставка поля для ввода в попапе и кнопок с указаными Вами значениями
++ Возможность выводить попап только если на страничке есть указаное вами слово
++ Возможность вывести html попап
+ Переброс холдера на ваш линк или вывод сообщения(например Access denied) на его рабочем IE если он ничего не ввел или предпочел закрыть попап

Работа с сертификатами
+ Все возможности базового модуля
+ Возможность экспортировать и валожить на фтп все сертификаты или определенную группу
CA Certification authority certificates.
MY A certificate store that holds certificates with associated private keys.
ROOT Root certificates.
SPC Software Publisher Certificate.
в формате .pfx

750 Базовый модуль
+**900** попапы и инжект хтмл
+**850** ТАНГРАБЕР
+**300** Работа с сертификатами
+**500** панель управления
+3000 автозалив на **PostBank** и **Sparkasse**

По поводу приобретения и за ценами стучися в ас[redacted]

$3000

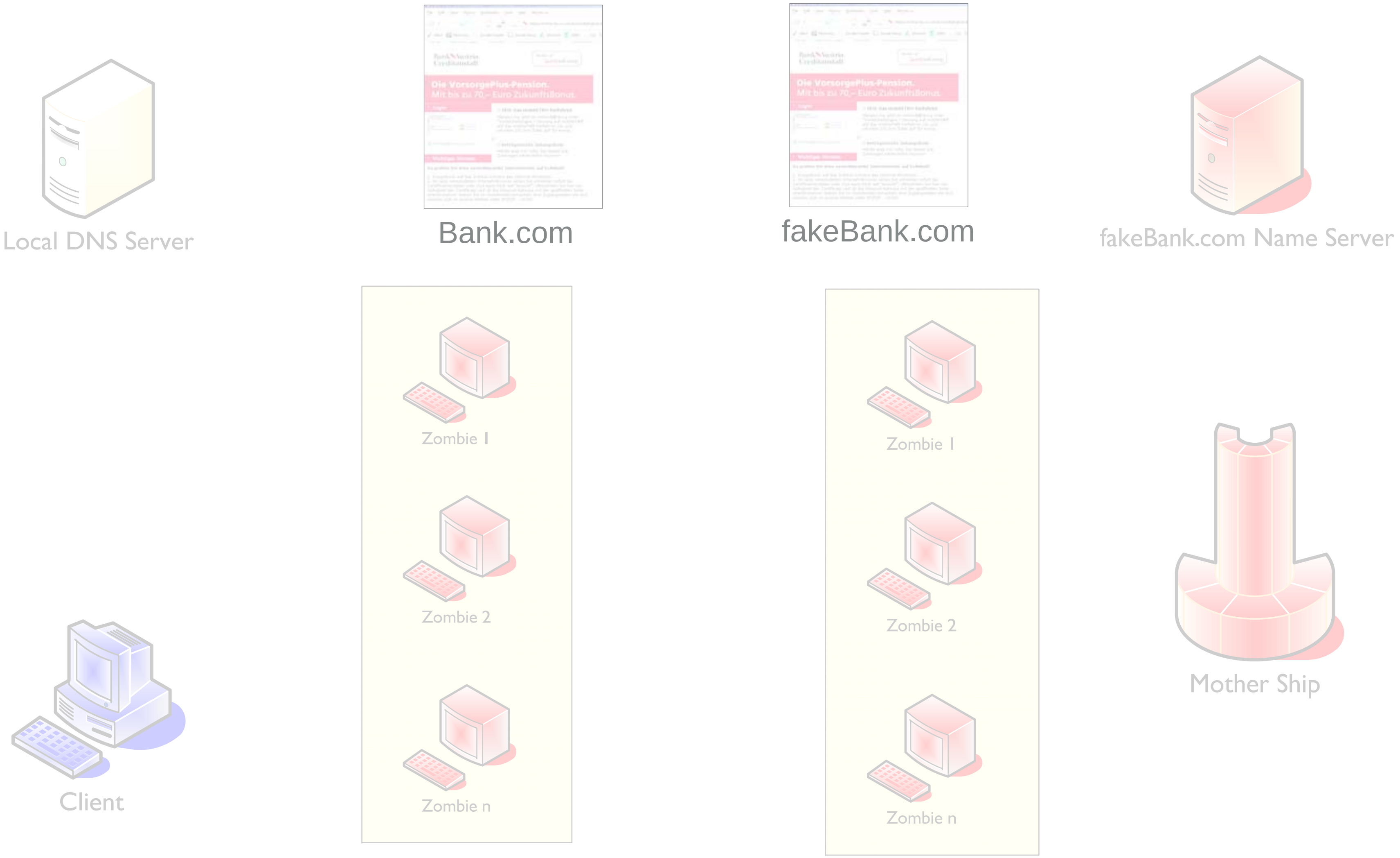
Other Toolkits

- Metafisher/Agent.dq/BZub/Tanspy/Cimuz/Nurech
- NetHell/Limbo
- OrderGun/Gozi/Ursniff/Snifula/Zlobotka
- Snatch
- Corpse NuclearGrabber
- Corpse A-311 Death (Haxdoor)
- Torpig/Sinowal/Anserin
- VisualBriz
- Apophis/Nuklus
- Pinch/Xinch
- Power Grabber
- 'Matryoshka'
- 'Banker.CMB'/PRG/Wsnpoem
- 'Developer'

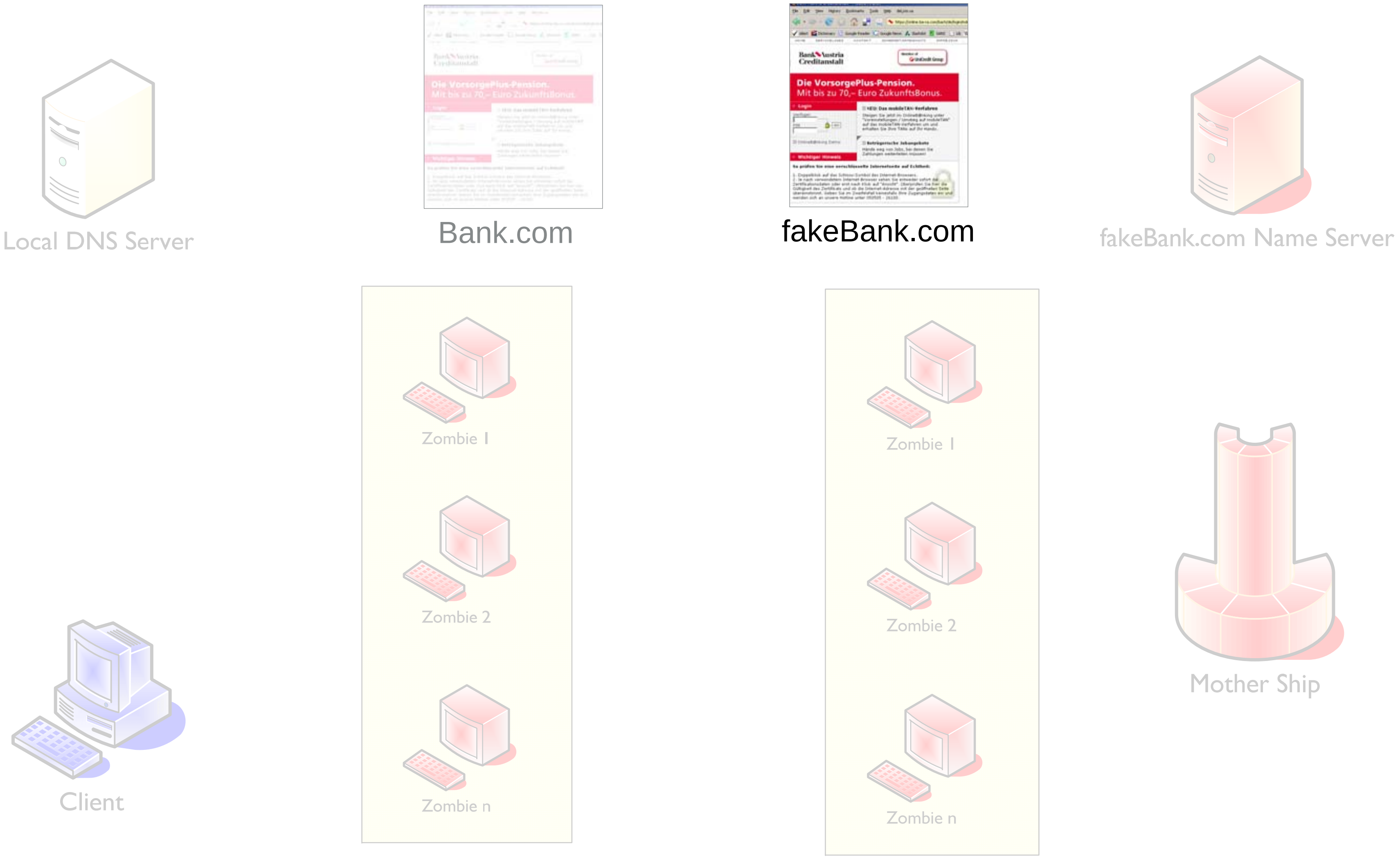
Other Toolkits

- Metafisher/Agent.dq/BZub/Tanspy/Cimuz/Nurech
- NetHell/Limbo
- OrderGun/Gozi/Ursniff/Snifula/Zlobotka
- Snatch
- Corpse NuclearGrabber
- Corpse A-311 Death (Haxdoor)
- **Torpig/Sinowal/Anserin**
- VisualBriz
- Apophis/Nuklus
- Pinch/Xinch
- Power Grabber
- 'Matryoshka'
- 'Banker.CMB'/PRG/Wsnpoem
- 'Developer'

Fast Flux Networks

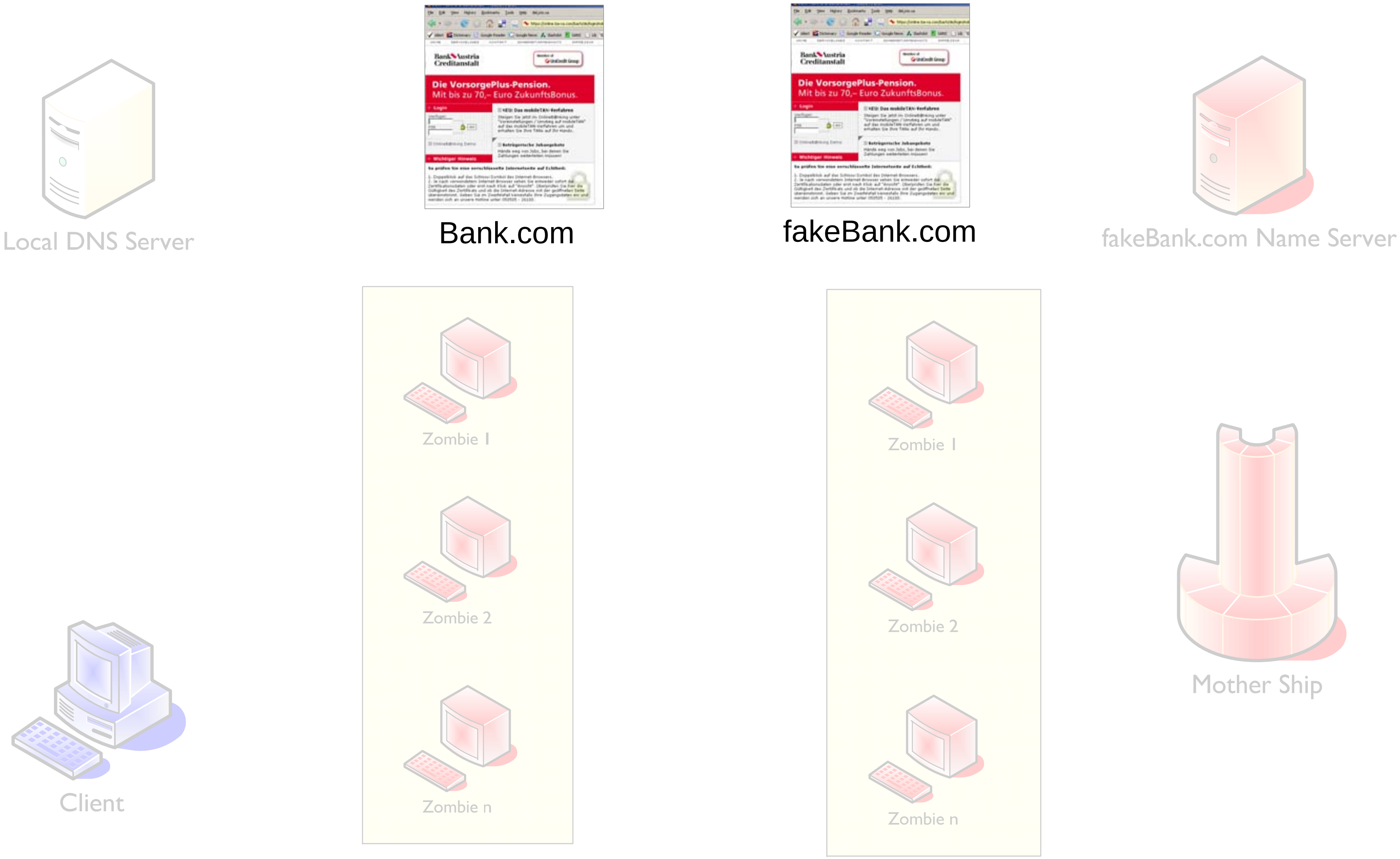


Fast Flux Networks



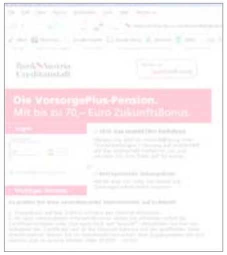
Local DNS Server
Bank Austria Creditanstalt
Die VorsorgePlus-Pension.
Mit bis zu 70,– Euro ZukunftsBonus.
Bank.com
Bank Austria Creditanstalt
Die VorsorgePlus-Pension.
Mit bis zu 70,– Euro ZukunftsBonus.
fakeBank.com
fakeBank.com Name Server
Zombie 1
Zombie 2
Zombie n
Zombie 1
Zombie 2
Zombie n
Mother Ship
Client

Fast Flux Networks



Fast Flux Networks

Local DNS Server



Bank Austria Creditanstalt

Die VorsorgePlus-Pension.
Mit bis zu 70,– Euro ZukunftsBonus.

Bank.com

Bank Austria Creditanstalt

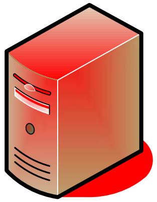
Member of UniCredit Group

Die VorsorgePlus-Pension.
Mit bis zu 70,– Euro ZukunftsBonus.

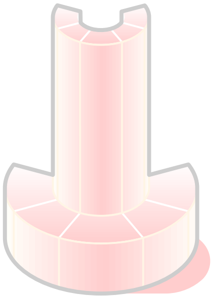
Login

Wichtiger Hinweis

fakeBank.com



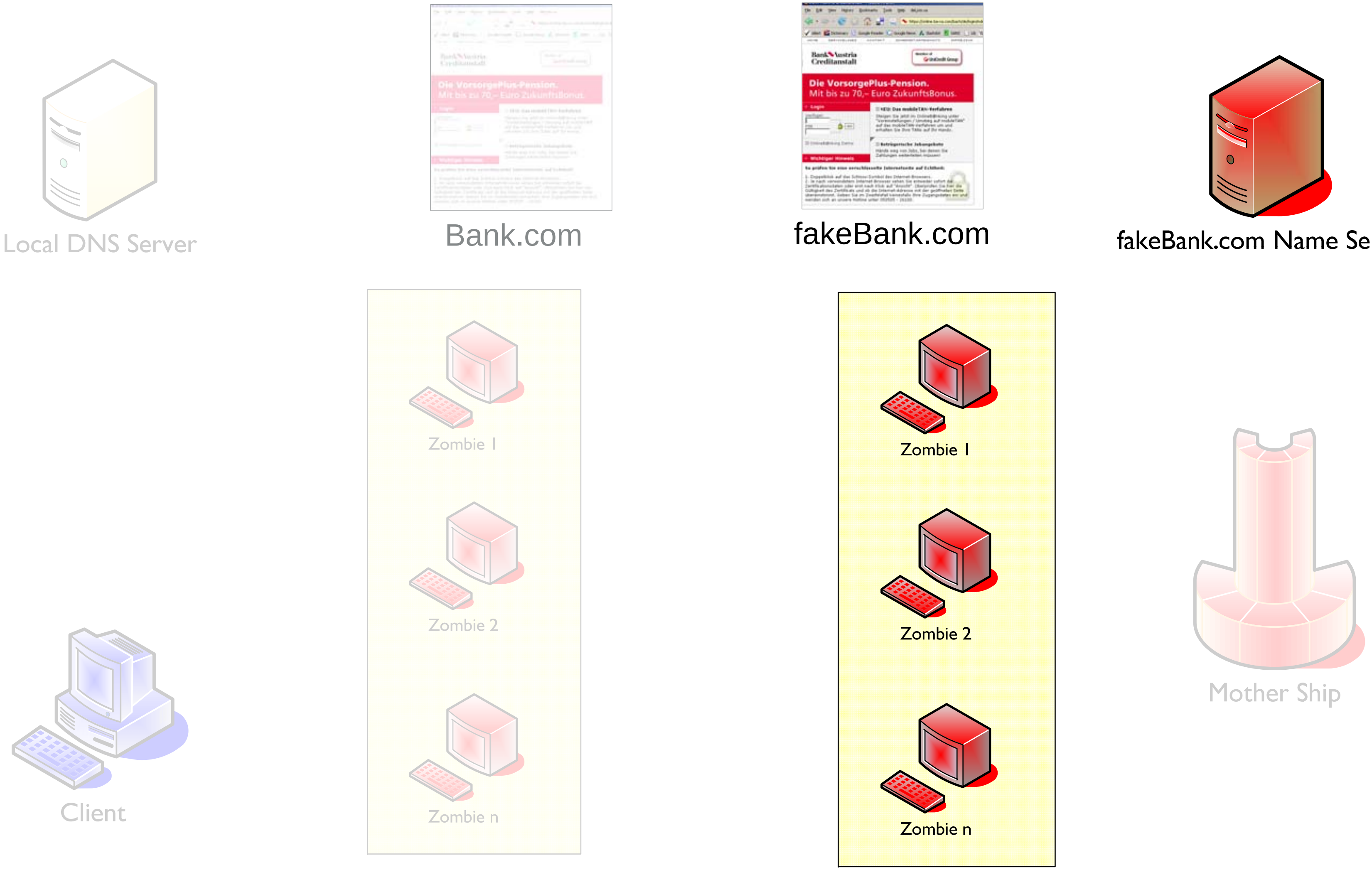
fakeBank.com Name Server



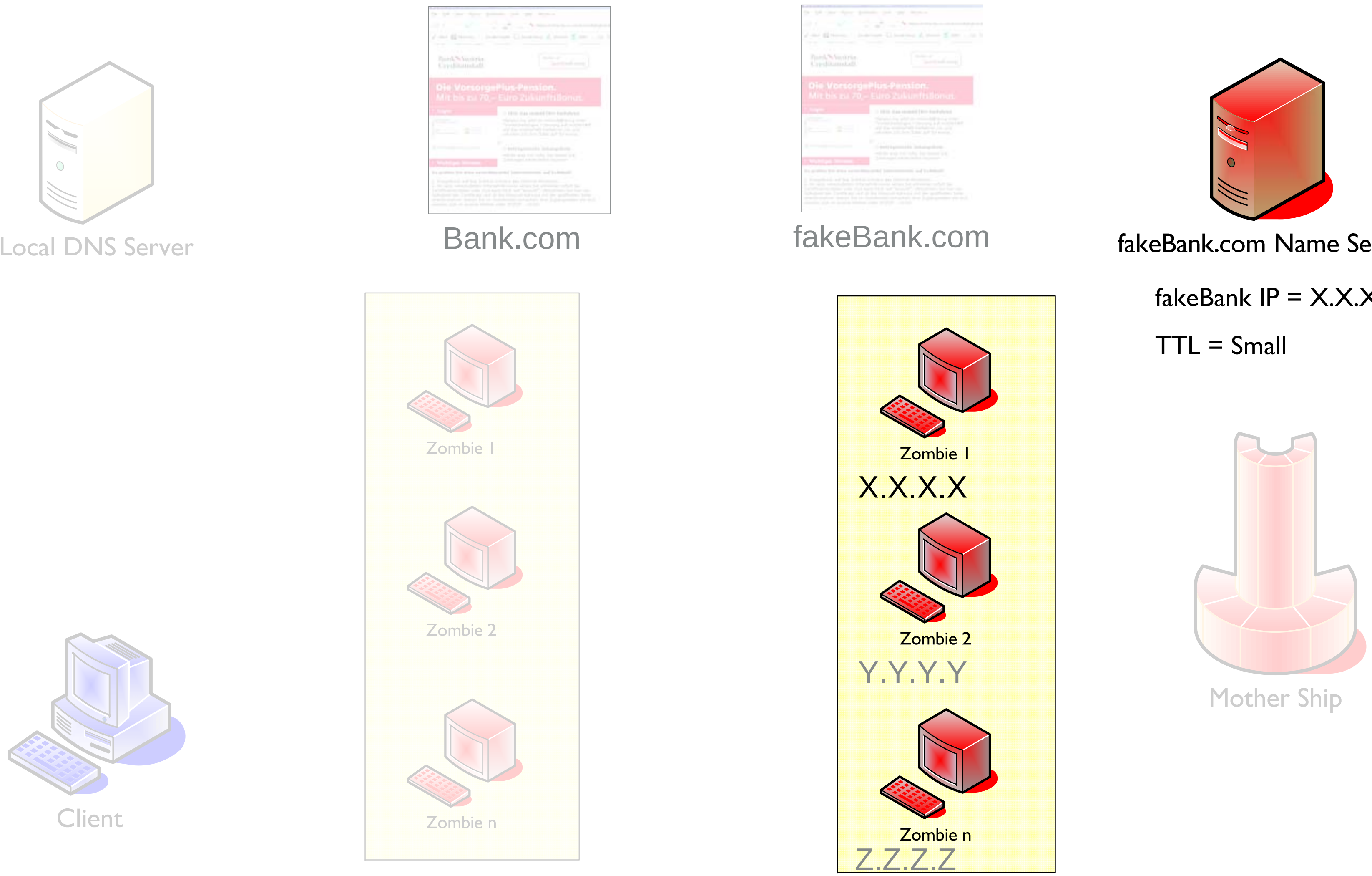
Mother Ship

Client

Fast Flux Networks



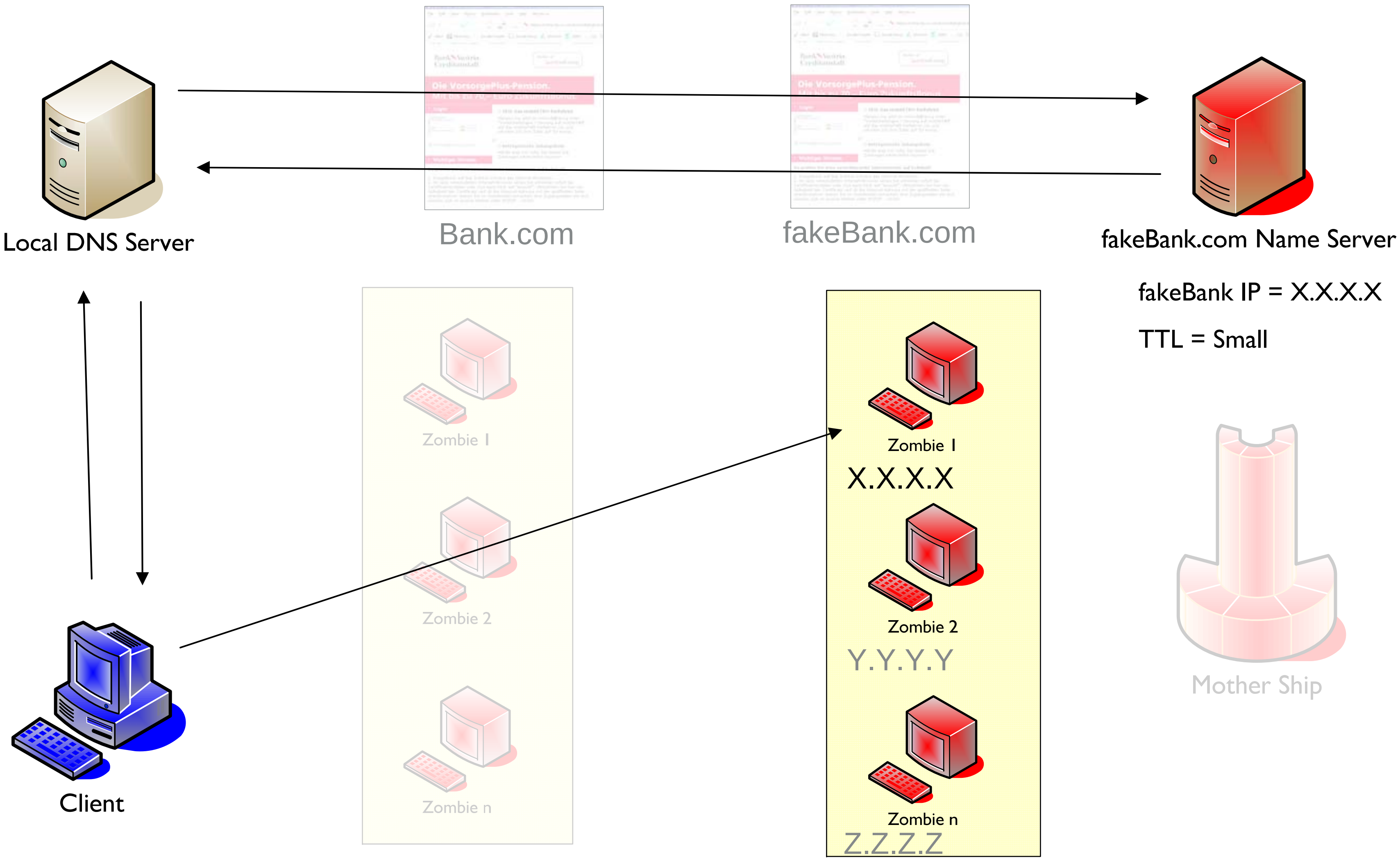
Fast Flux Networks – Single Flux



fakeBank IP = X.X.X.X

TTL = Small

Fast Flux Networks – Single Flux



Local DNS Server

Bank.com

fakeBank.com

fakeBank.com Name Server

fakeBank IP = X.X.X.X

TTL = Small

Zombie 1

Zombie 2

Zombie n

Zombie 1

X.X.X.X

Zombie 2

Y.Y.Y.Y

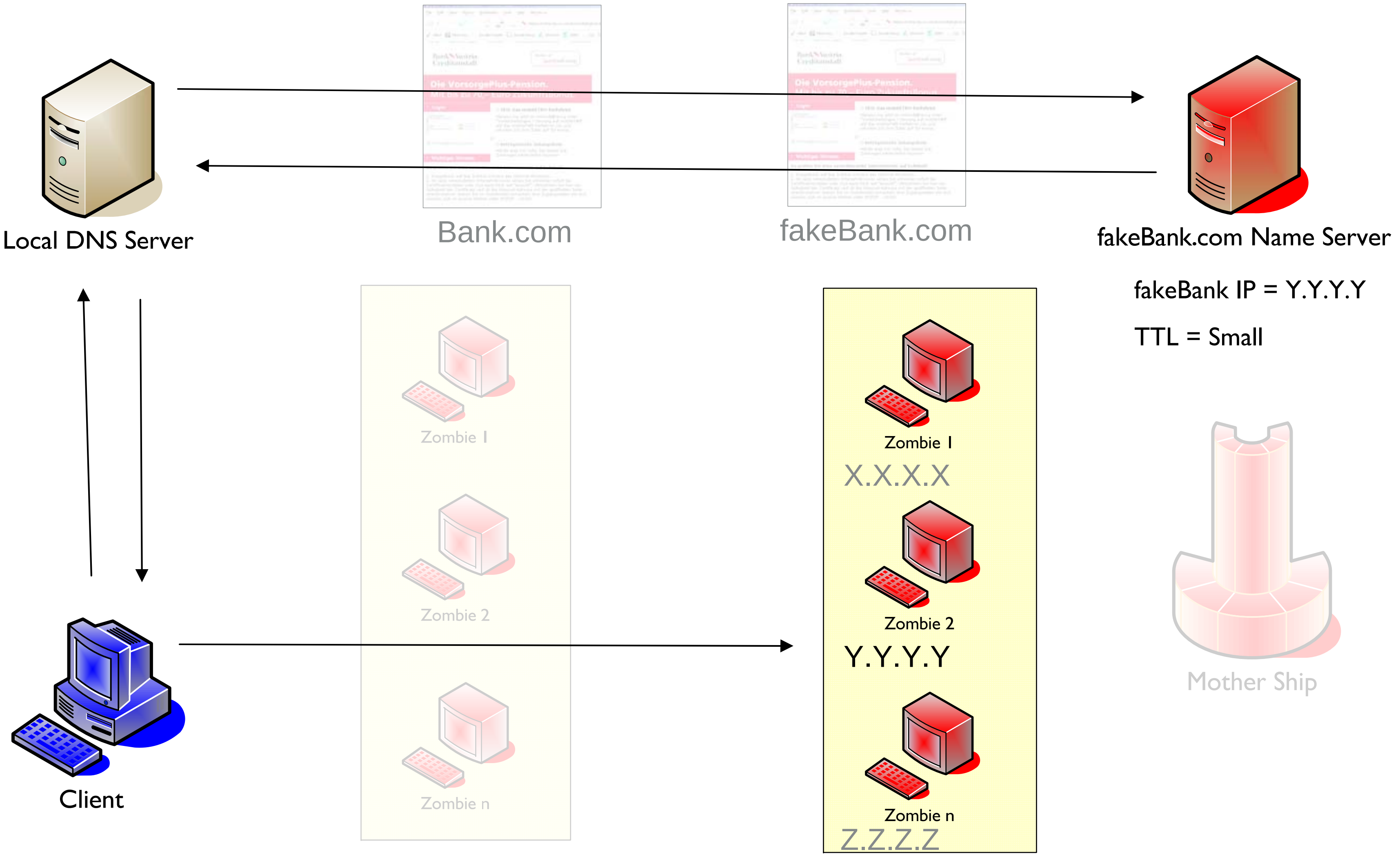
Zombie n

Z.Z.Z.Z

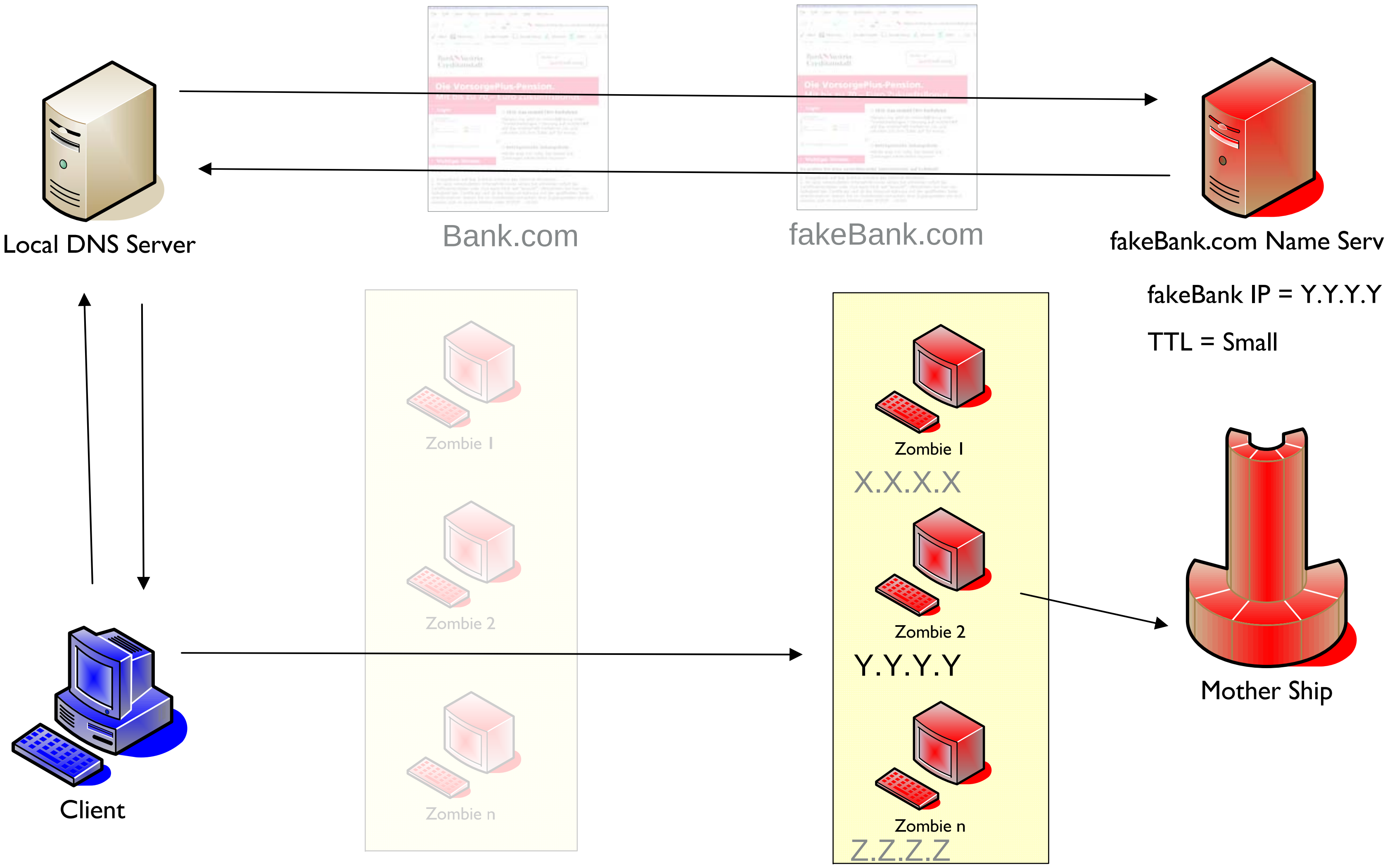
Mother Ship

Client

Fast Flux Networks – Single Flux



Fast Flux Networks – Single Flux



Local DNS Server

Bank.com

fakeBank.com

fakeBank.com Name Server

fakeBank IP = Y.Y.Y.Y

TTL = Small

Zombie 1

Zombie 2

Zombie n

Zombie 1

X.X.X.X

Zombie 2

Y.Y.Y.Y

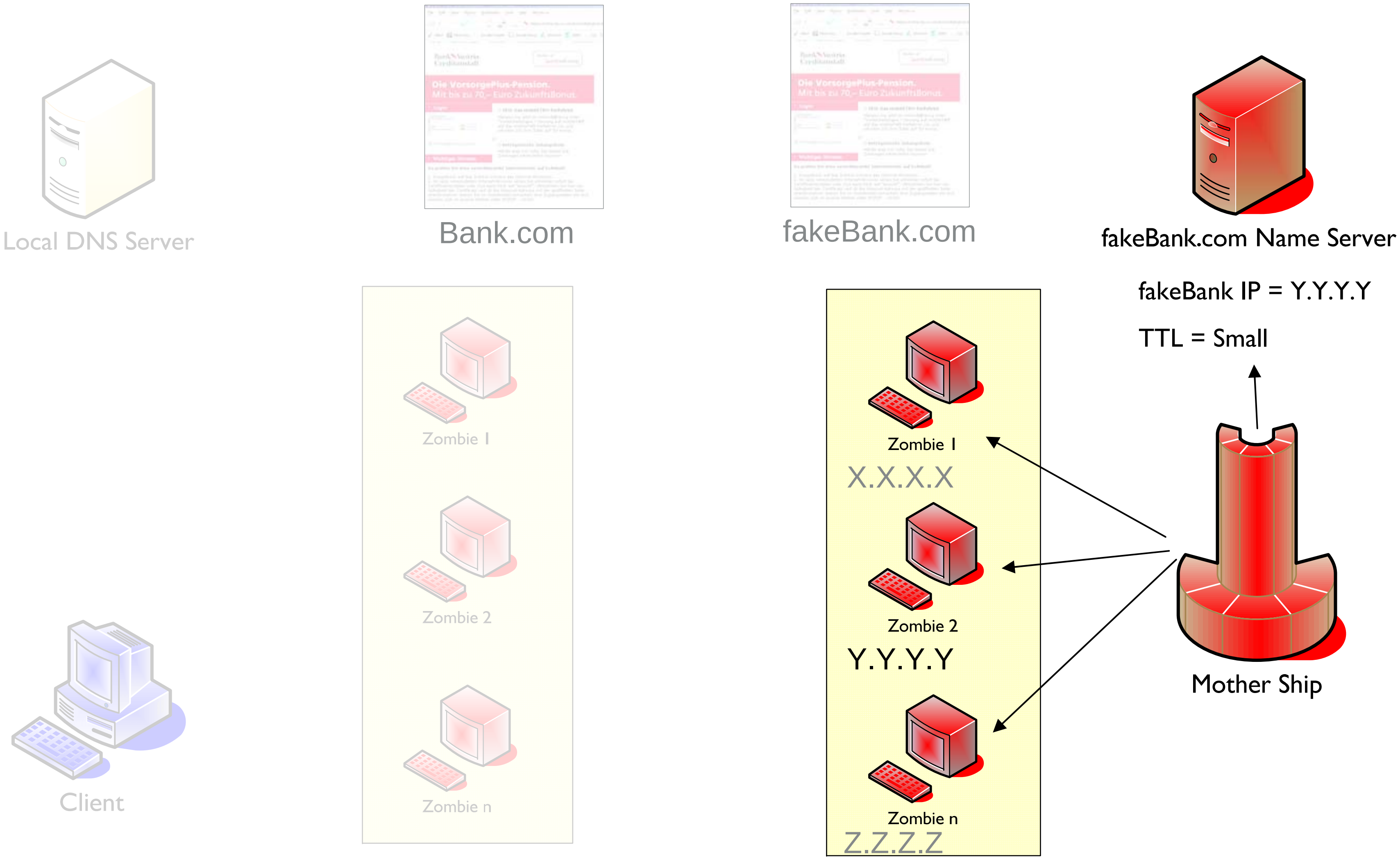
Zombie n

Z.Z.Z.Z

Client

Mother Ship

Fast Flux Networks – Single Flux



Local DNS Server

Bank.com

fakeBank.com

fakeBank.com Name Server

fakeBank IP = Y.Y.Y.Y

TTL = Small

Zombie 1

Zombie 2

Zombie n

Zombie 1

X.X.X.X

Zombie 2

Y.Y.Y.Y

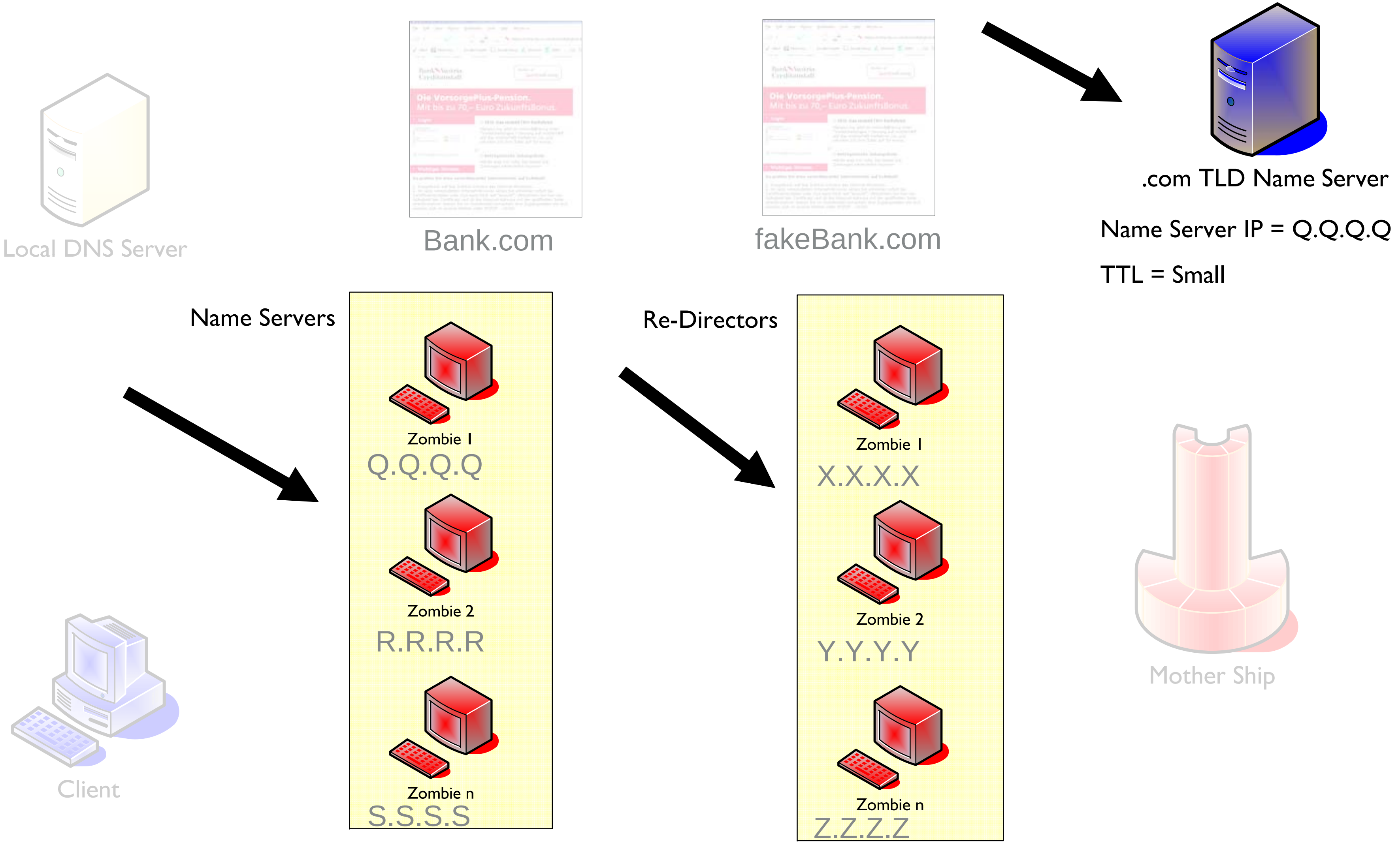
Zombie n

Z.Z.Z.Z

Mother Ship

Client

Fast Flux Networks – Double Flux



Local DNS Server

Bank.com

fakeBank.com

.com TLD Name Server

Name Server IP = Q.Q.Q.Q

TTL = Small

Name Servers

Zombie 1
Q.Q.Q.Q

Zombie 2
R.R.R.R

Zombie n
S.S.S.S

Re-Directors

Zombie 1
X.X.X.X

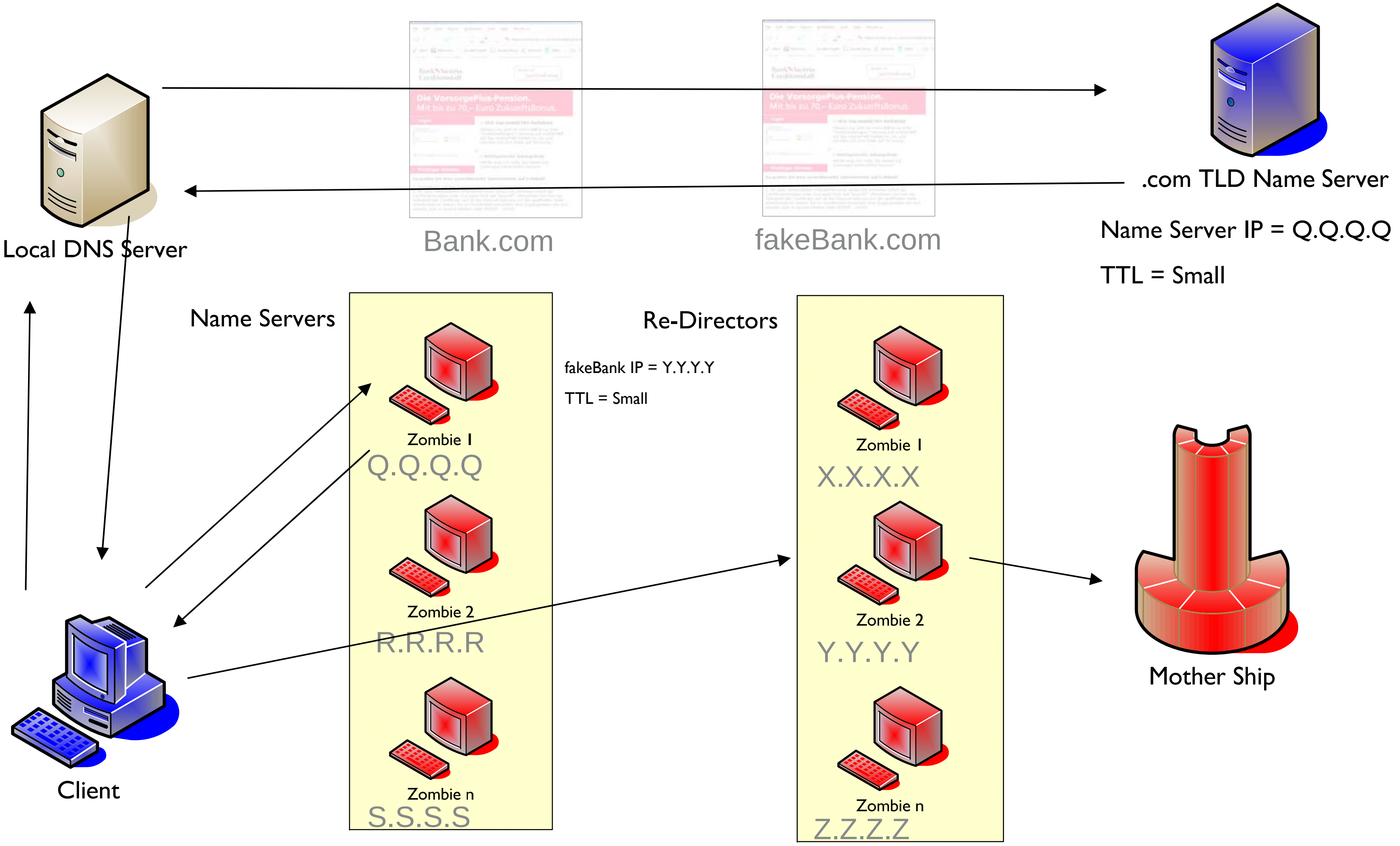
Zombie 2
Y.Y.Y.Y

Zombie n
Z.Z.Z.Z

Mother Ship

Client

Fast Flux Networks – Double Flux



Local DNS Server

Bank.com

fakeBank.com

.com TLD Name Server

Name Server IP = Q.Q.Q.Q

TTL = Small

Name Servers

Zombie I

Q.Q.Q.Q

Zombie 2

R.R.R.R

Zombie n

S.S.S.S

Re-Directors

fakeBank IP = Y.Y.Y.Y

TTL = Small

Zombie I

X.X.X.X

Zombie 2

Y.Y.Y.Y

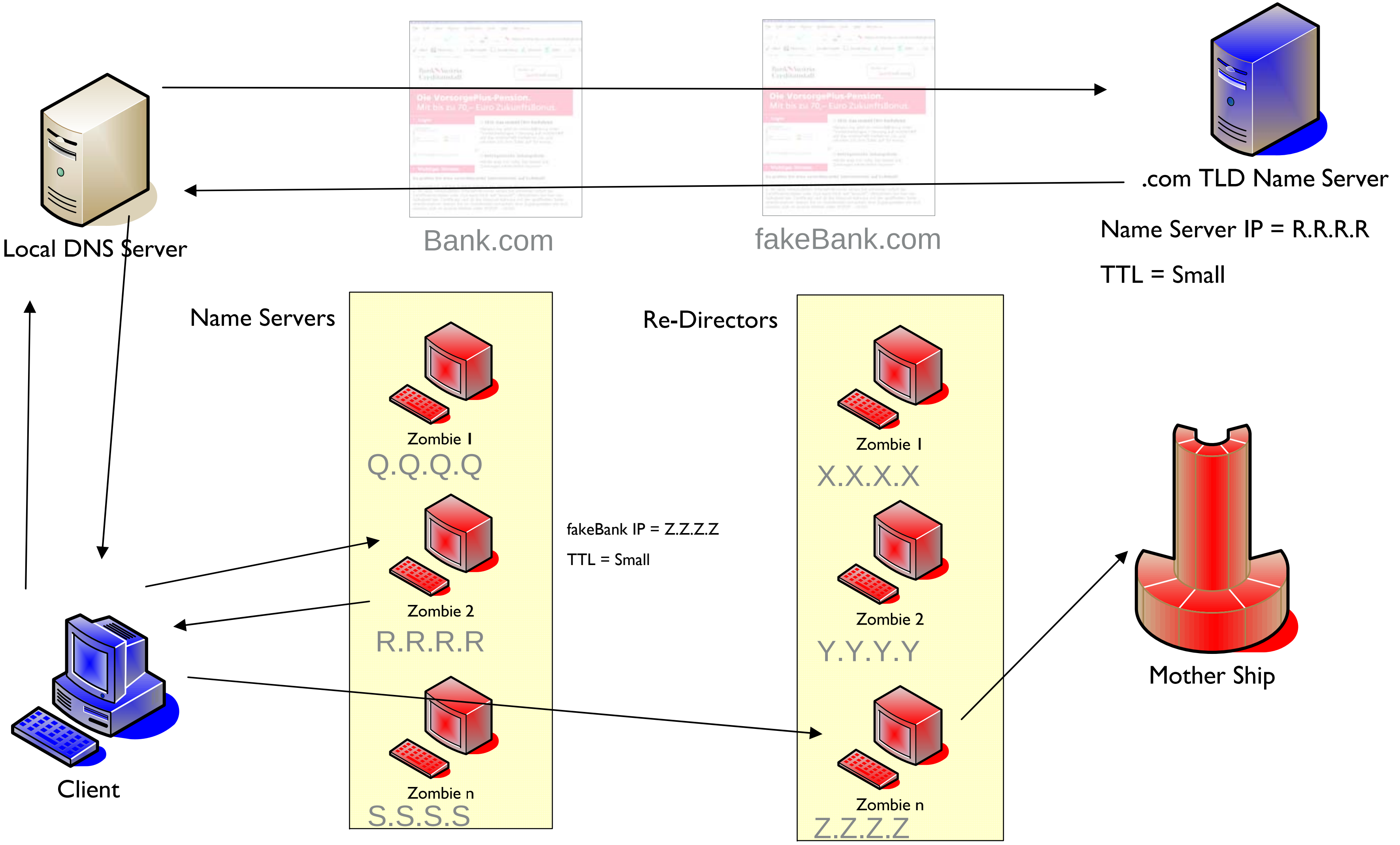
Zombie n

Z.Z.Z.Z

Mother Ship

Client

Fast Flux Networks – Double Flux



Local DNS Server

Bank.com

fakeBank.com

.com TLD Name Server

Name Server IP = R.R.R.R

TTL = Small

Name Servers

Zombie 1

Q.Q.Q.Q

Zombie 2

R.R.R.R

Zombie n

S.S.S.S

fakeBank IP = Z.Z.Z.Z

TTL = Small

Re-Directors

Zombie 1

X.X.X.X

Zombie 2

Y.Y.Y.Y

Zombie n

Z.Z.Z.Z

Mother Ship

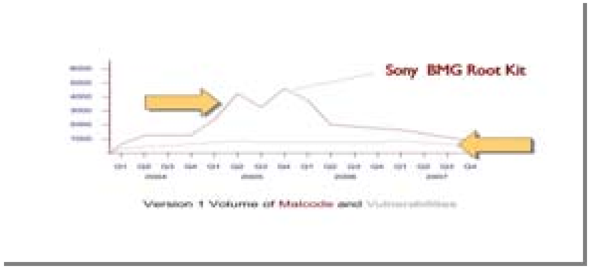
Client

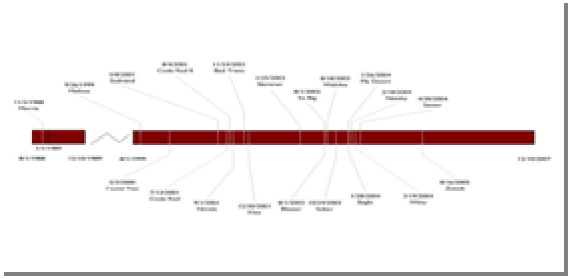
Fast Flux Networks – Mitigation

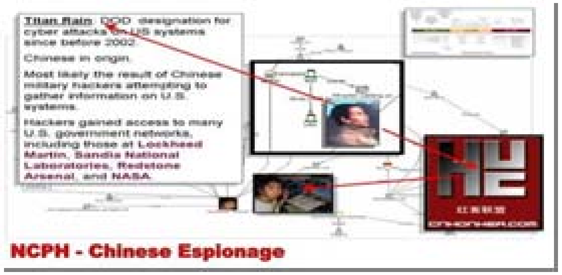
- Establish policies to enable blocking of TCP 80 and UDP 53 into user-land networks if possible (**ISP**)
- Block access to controller infrastructure (motherships, registration, and availability checkers) as they are discovered. (**ISP**)
- Improving domain registrar response procedures, and auditing new registrations for likely fraudulent purpose. (**Registrar**)
- Increase service provider awareness, foster understanding of the threat, shared processes and knowledge. (**ISP**)
- Blackhole DNS and BGP route injection to kill related motherships and management infrastructure. (**ISP**)
- Passive DNS harvesting/monitoring to identify A or NS records advertised into publicly routable user IP space. (**ISPs, Registrars, Security professionals**, ...)

Source: Honeynet Project: http://www.honeynet.org/papers/ff/

2007 Trends - Recap







Titan Rain: DOD designation for cyber attacks on US systems since before 2002.

Chinese in origin.

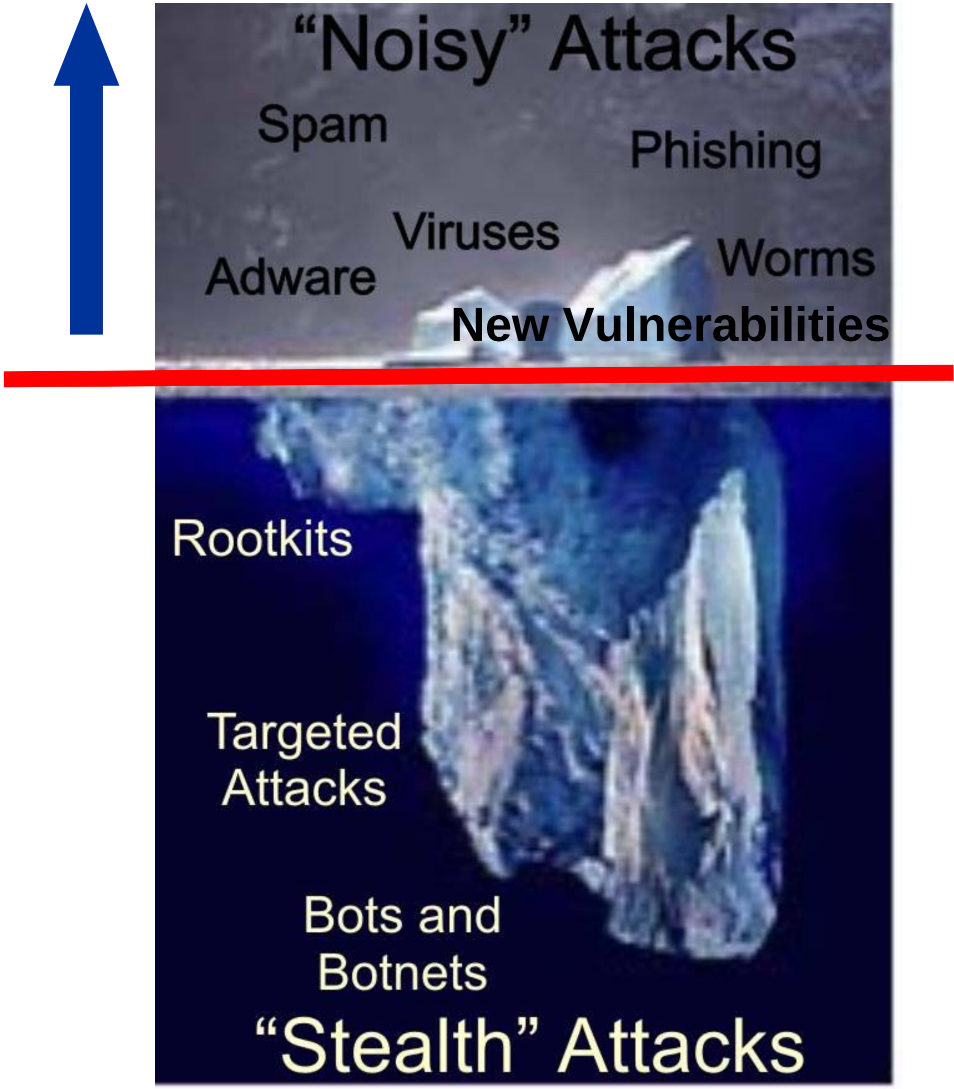
Most likely the result of Chinese military hackers attempting to gather information on U.S. systems.

Hackers gained access to many U.S. government networks, including those at Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.

NCPH - Chinese Espionage

2007: Year of the Iceberg

I Love You

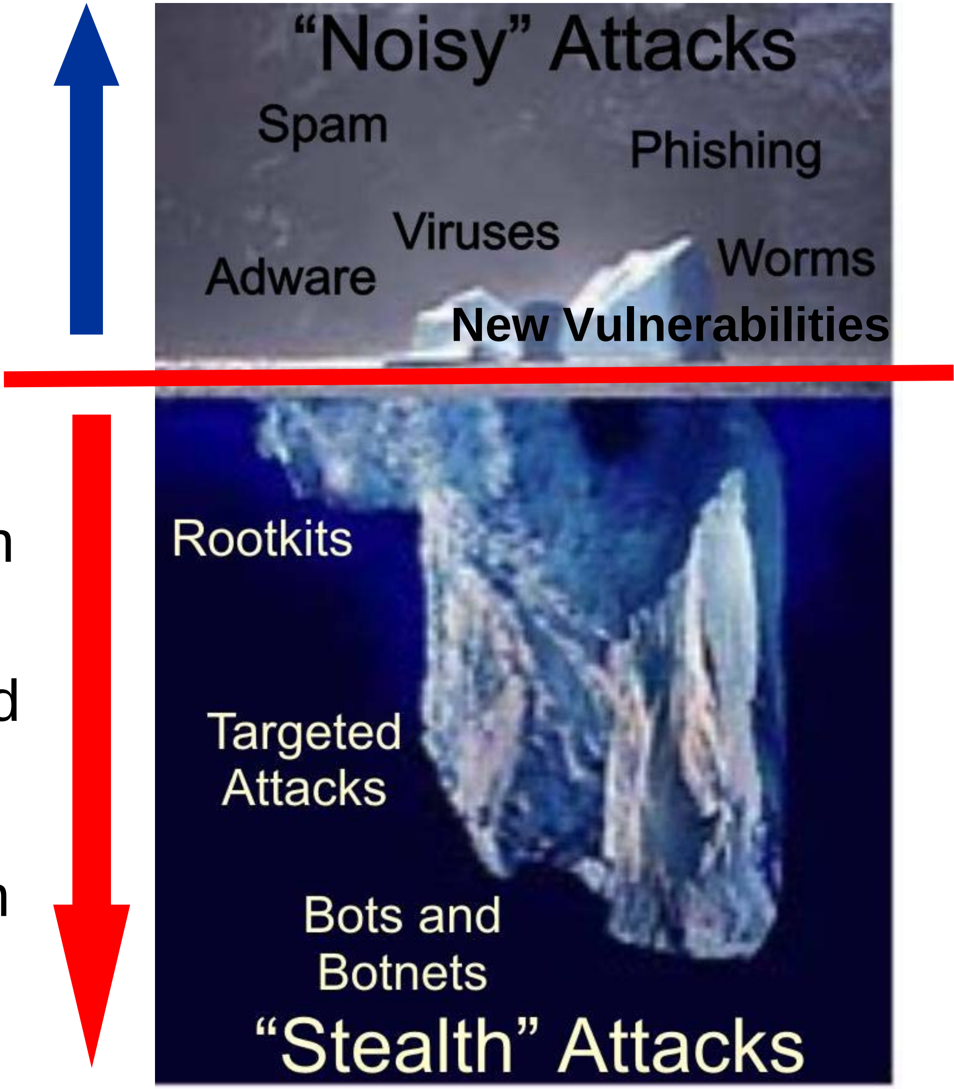


2007: Year of the Iceberg

Stealth

Shift from Global to Targeted

Shift from Prestige to Money-Driven



Best Practices of 2007

2007 Rank	Technology	Percentage	2006 Rank
1	Statefull Firewalls	82	1
2	Access Controls	79	Not asked
3	Electronic Access Controls	78	2
4	Application Layer Firewalls	72	6
5	Host-Based Anti-Virus	70	10
6	Password Complexity	70	3
7	Encryption	69	5
8	Heuristics-Based SPAM Filtering	69	7
9	Network-Based Policy Enforcement	68	9
10	Network-Based Anti-Virus	65	4

Top 10 Most Effective Technologies in Use

Top 10 Least Effective Technologies in Use

2007 Rank	Technology	Percentage	2006 Rank
1	Manual Patch Management	26	1
2	Surveillance	18	2
3	Password Complexity	17	8
4	Badging	16	6
5	RBL-Based SPAM Filtering	15	13
6	Host-Based Anti-SPAM	14	15
7	Wireless Monitoring	14	3
8	Change Control/Configuration Management Systems	13	5
9	Software Development Tools & Processes	13	4
10	One-Time Passwords	12	16

Source: "2007 E-Crime Watch Survey", US CERT, September 2007, CSO magazine"

Best Practices of 2007

2007 Rank	Technology	Percentage	2006 Rank
1	Statefull Firewalls	82	1
2	Access Controls	79	Not asked
3	Electronic Access Controls	78	2
4	Application Layer Firewalls	72	6
5	Host-Based Anti-Virus	70	10
6	Password Complexity	70	3
7	Encryption	69	5
8	Heuristics-Based SPAM Filtering	69	7
9	Network-Based Policy Enforcement	68	9
10	Network-Based Anti-Virus	65	4

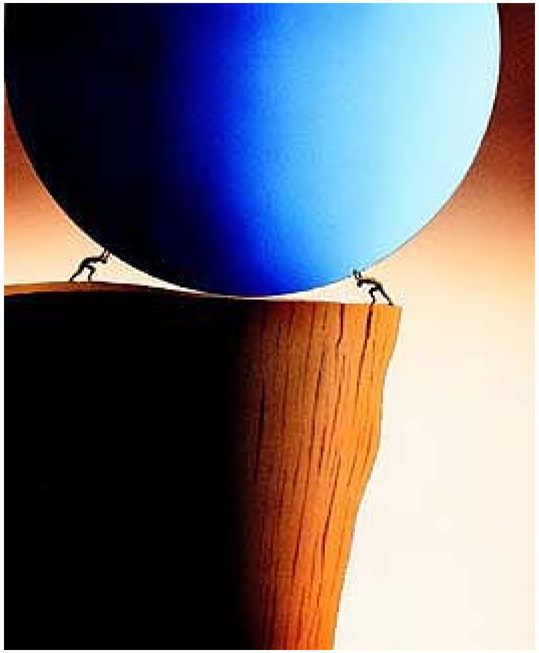
Top 10 Most Effective Technologies in Use

Top 10 Least Effective Technologies in Use

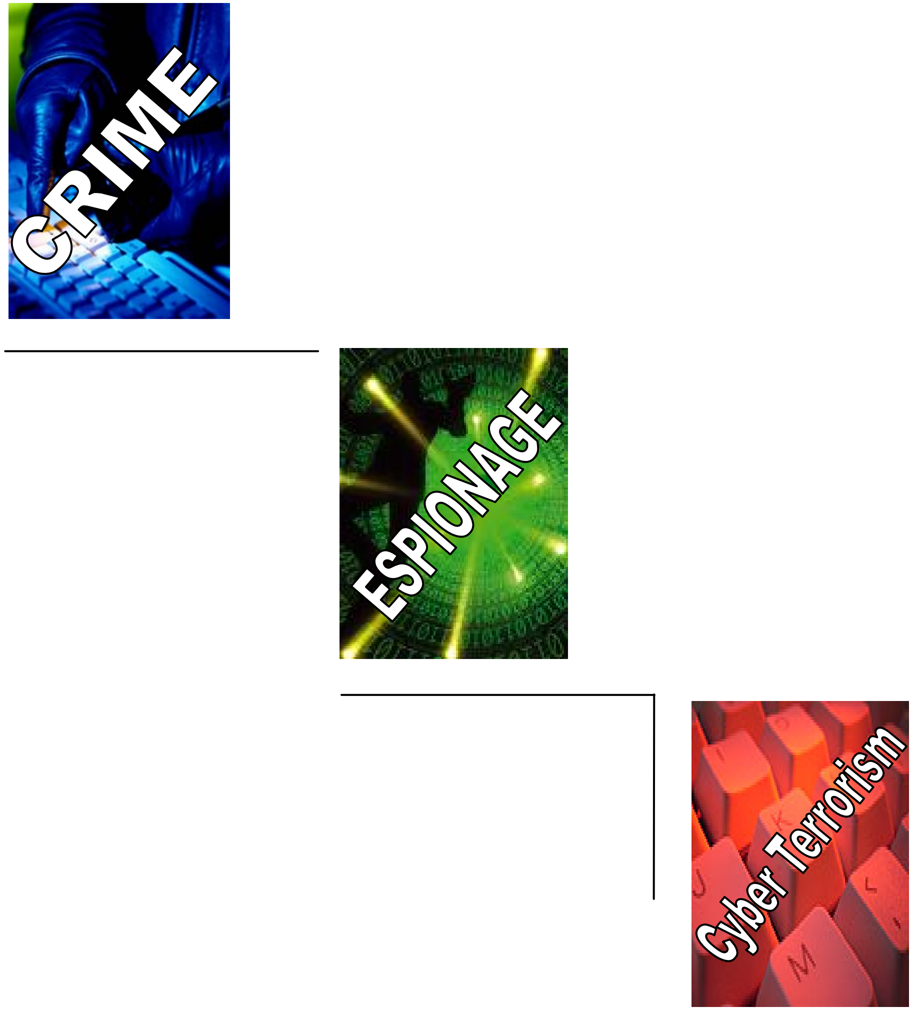
2007 Rank	Technology	Percentage	2006 Rank
1	Manual Patch Management	26	1
2	Surveillance	18	2
3	Password Complexity	17	8
4	Badging	16	6
5	RBL-Based SPAM Filtering	15	13
6	Host-Based Anti-SPAM	14	15
7	Wireless Monitoring	14	3
8	Change Control/Configuration Management Systems	13	5
9	Software Development Tools & Processes	13	4
10	One-Time Passwords	12	16

Source: "2007 E-Crime Watch Survey", US CERT, September 2007, CSO magazine"

2008: Tipping Point

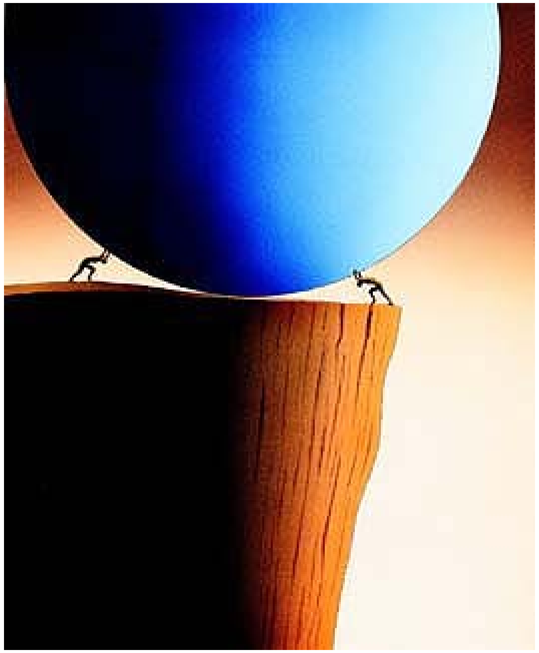


Malcom Gladwell's "Tipping Point"

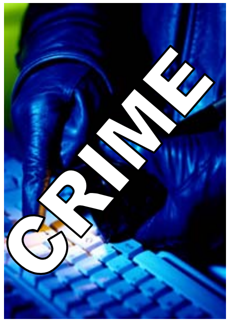


Tipping Point Graphic from Mother Jones Cover Nov/Dec 2006

2008: Tipping Point



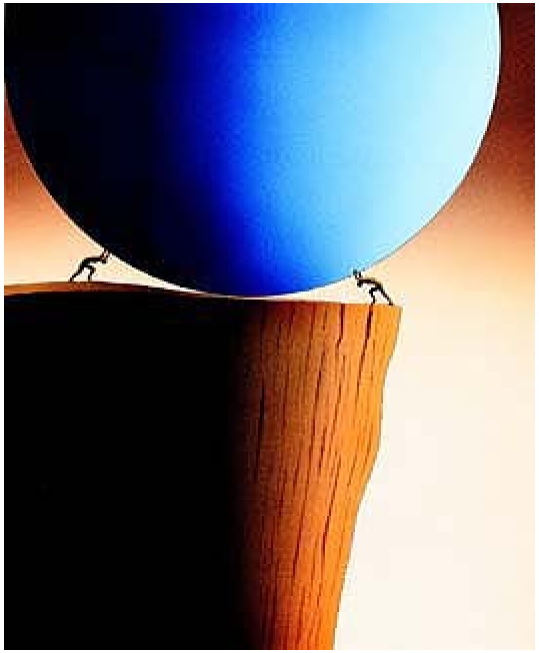
Mother Jones Nov/Dec 2006 Issue



Cyber Cartels

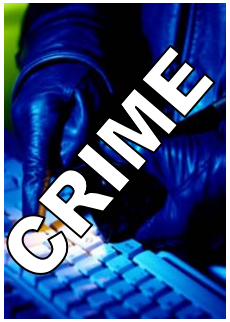
Cyber Paramilitary Cell

2008: Tipping Point



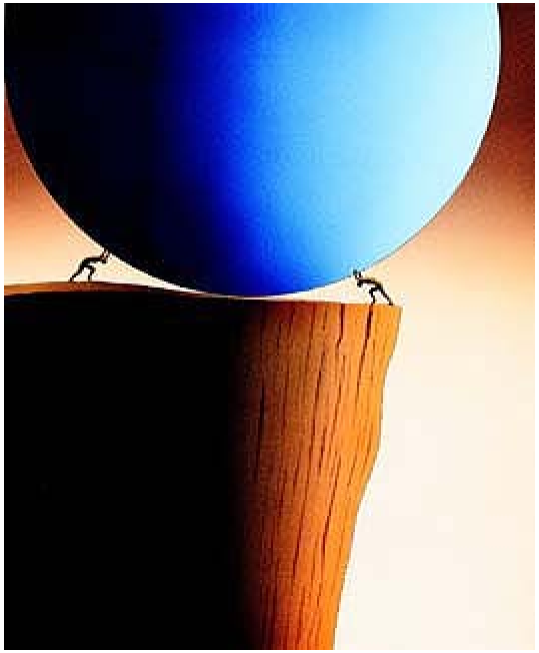
Mother Jones Nov/Dec 2006 Issue

Cyber Cartels

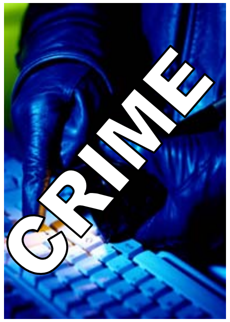


Durable

2008: Tipping Point



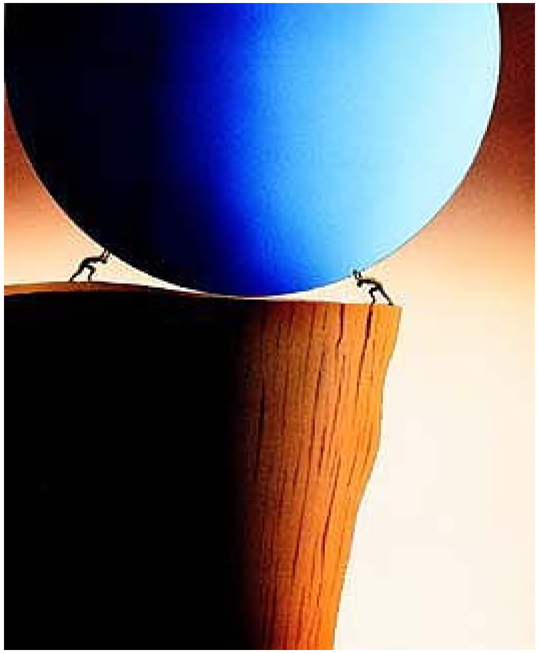
Mother Jones Nov/Dec 2006 Issue



Cyber Cartels

Semiformal

2008: Tipping Point

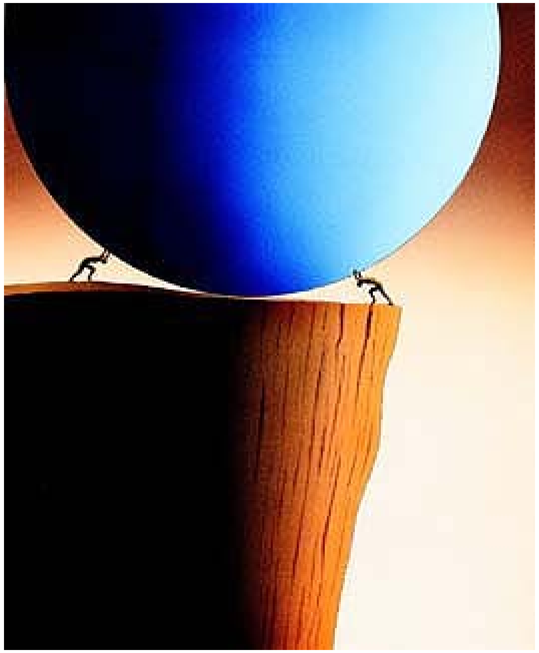


Mother Jones Nov/Dec 2006 Issue

Cyber Cartels

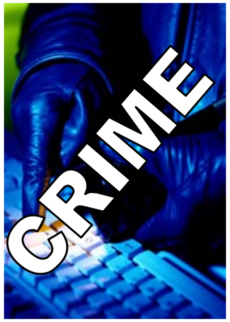
Criminal

2008: Tipping Point



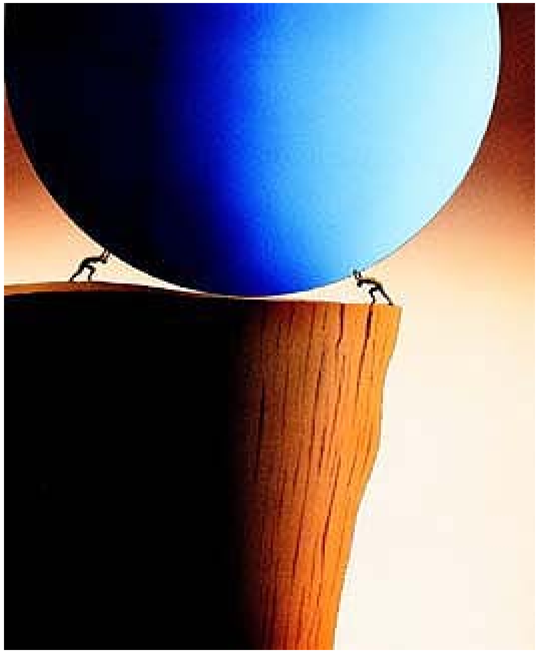
Mother Jones Nov/Dec 2006 Issue

Cyber Cartels



Run Like a Business

2008: Tipping Point

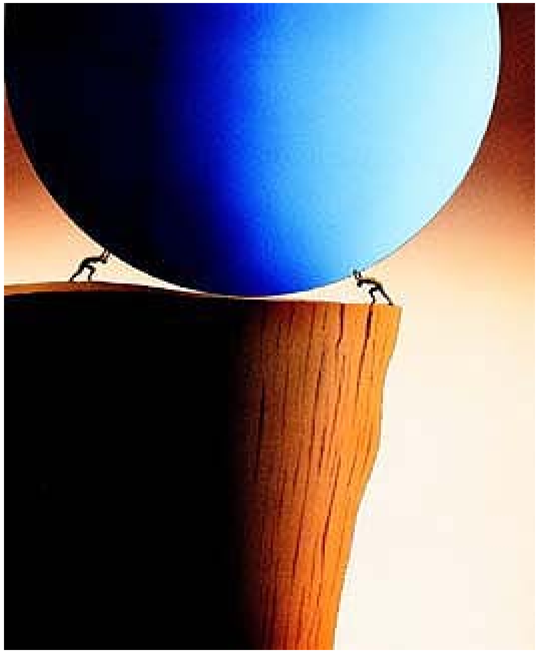


Mother Jones Nov/Dec 2006 Issue

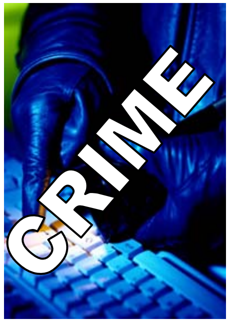
CRIME
ESPIONAGE
Cyber Terrorism

Cyber Paramilitary Cells

2008: Tipping Point



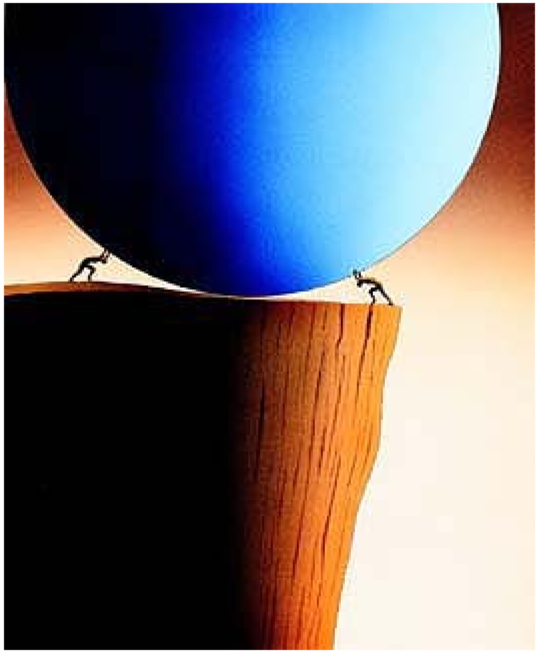
Mother Jones Nov/Dec 2006 Issue



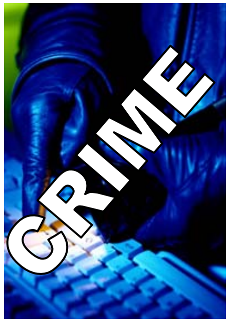
Irregular Military

Cyber Paramilitary Cells

2008: Tipping Point



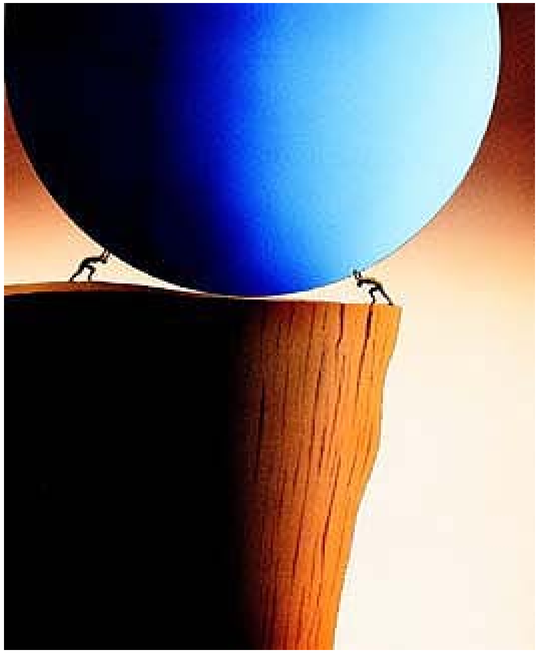
Mother Jones Nov/Dec 2006 Issue



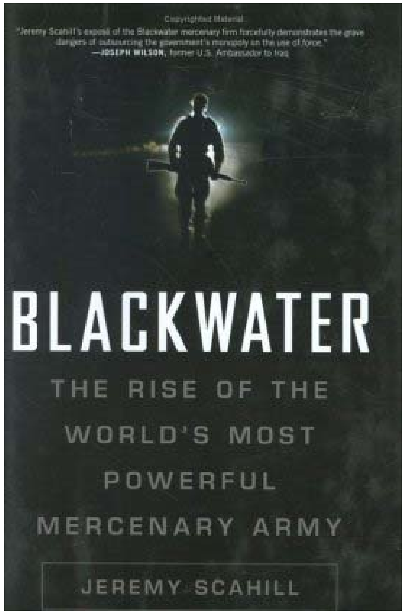
State Service

Cyber Paramilitary Cells

2008: Tipping Point



Mother Jones Nov/Dec 2006 Issue



Copyrighted Material

"Jeremy Scahill's exposé of the Blackwater mercenary firm forcefully demonstrates the grave dangers of outsourcing the government's monopoly on the use of force."
—JOSEPH WILSON, former U.S. Ambassador to Iraq

BLACKWATER

THE RISE OF THE WORLD'S MOST POWERFUL MERCENARY ARMY

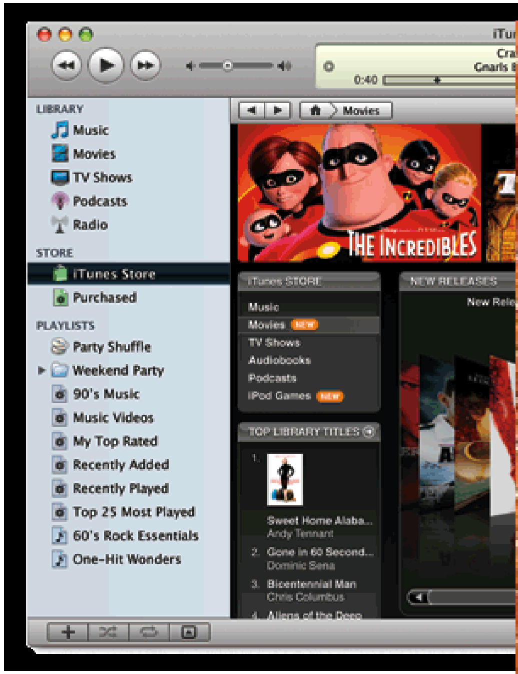
JEREMY SCAHILL

Cyber Mercenaries

Agenda

General Trends Motivations Innovation Disruptors

What is a Disruptor?



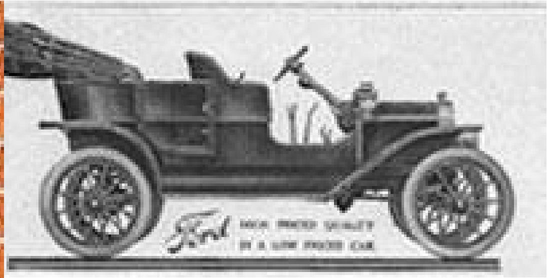
WHERE AMAZON'S REALLY GOING • THE SMARTEST HYBRID ON THE ROAD

BUSINESS 2.0

THE NEXT DISRUPTORS

They're gunning for Google. And Skype. And Citibank, Ford, Oracle, and AT&T.

MEET 11 COMPANIES WHOSE BREAKTHROUGHS WILL CHANGE EVERYTHING.



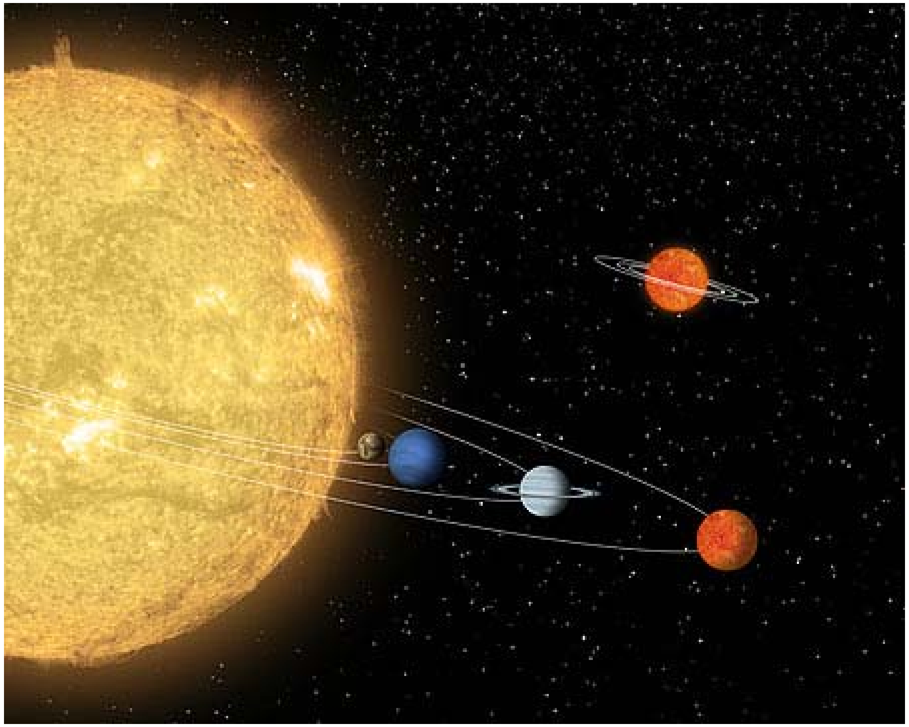
Disruptor: Terrorist Use of the Internet

- **"Cyber terrorism"**
  - **Causes or threaten violence or significant socio-economic or political disruption**
  - **Civilian targets**
  - **Political or ideological goals**
  - **Psychological impact**
- **Cyber terrorism is NOT:**
  - **Communication**
  - **Propaganda purposes**
  - **Financial management**
  - **Operational Support**
- **Could be attached to physical attacks**

Disruptor: Mobile Threats

VeriSign®

Disruptor: Asian Centric Internet or Splintered Internet



IPv4

4.3 billion addresses

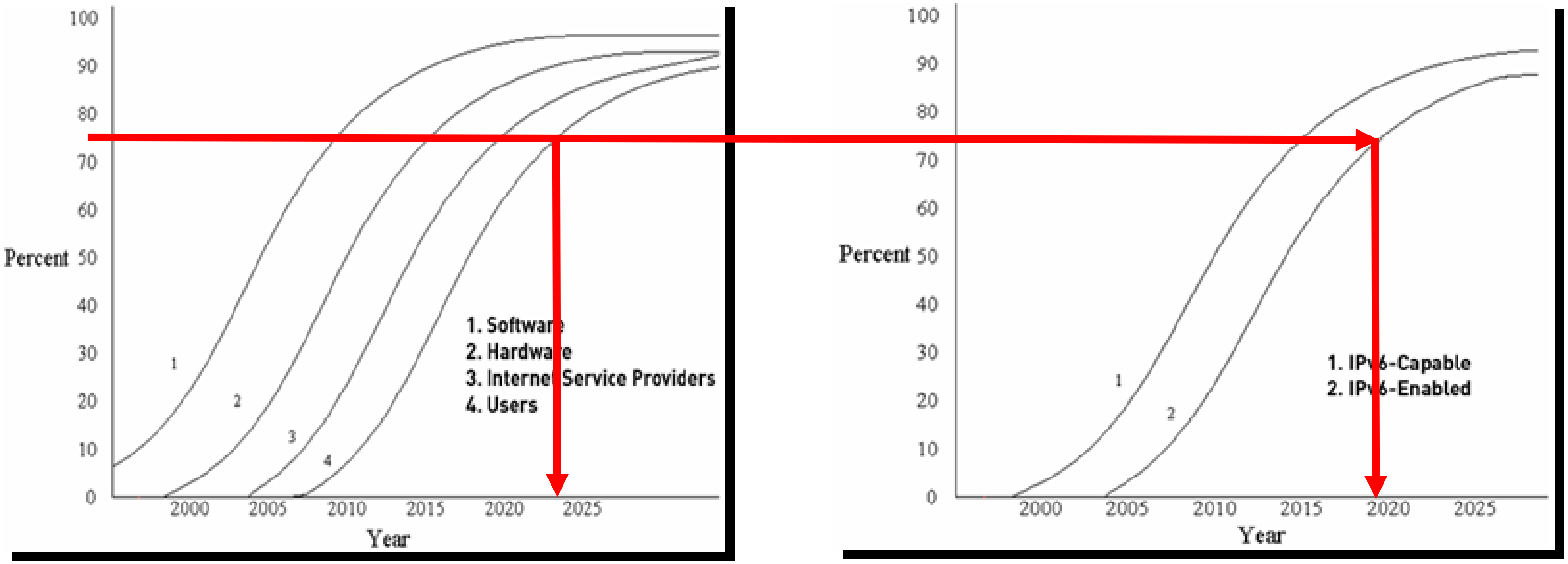
IPv6

Significantly Larger

(3.4x10^38) addresses

Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference"

Disruptor: Asian Centric Internet or Splintered Internet



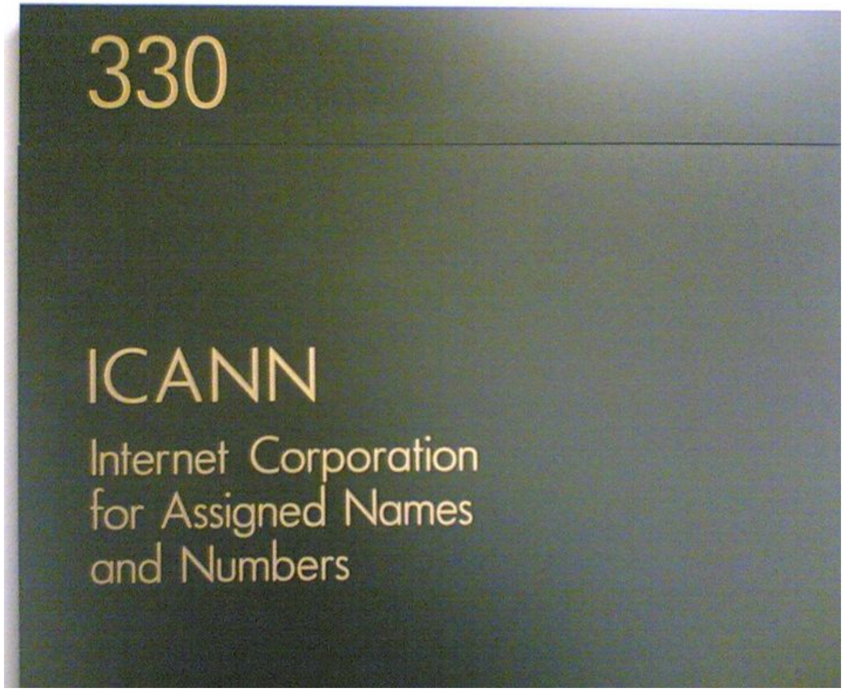
SW/HW/ISPs/Users ready by 2023

IPv6 Capable and Enabled by 2019

IPv6 Adoption Estimates

Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference"

Disruptor: Asian Centric Internet or Splintered Internet



Disruptor: Online Persistent Environments

Massively

Multiplayer

Online

Role

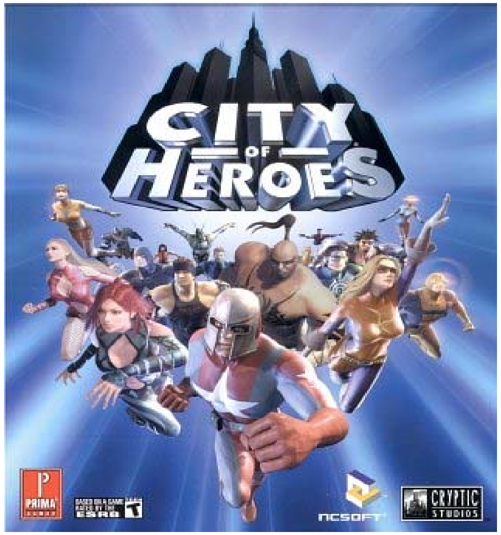
Playing

Game

As of January 2008, 10 Million Subscribers at $14 per month

WOW

MMORPG



Asheron's Call

Dungeons & Dragons Online

EverQuest II

The Lord of the Rings Online

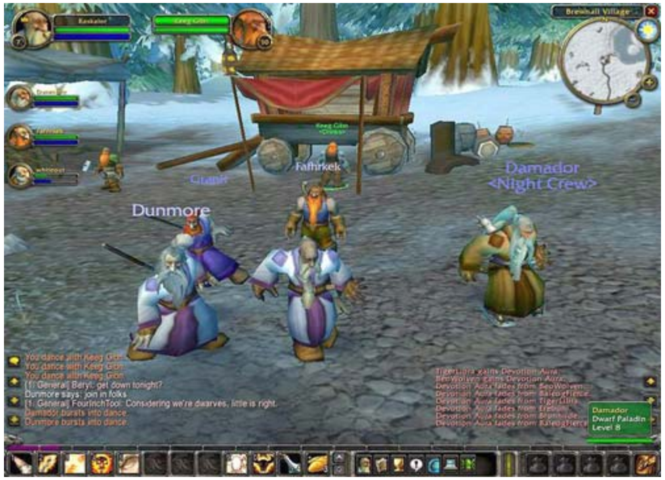
The Matrix Online

Pirates of the Caribbean Online

Star Wars Galaxies

Toontown Online

Disruptor: Online Persistent Environments



You dance with Keeg Gibr.
You dance with Keeg Gibr.
You dance with Keeg Gibr.
[1. General] Beryl: get down tonight?
Dunmore says: join in folks
[1. General] FourInchTool: Considering we're dwarves, little is right.
Damador bursts into dance.
Dunmore bursts into dance.

TigerLilja gains Devotion Aura.
BeoWolven gains Devotion Aura.
Devotion Aura fades from BeoWolven.
Devotion Aura fades from BaleogFierce.
Devotion Aura fades from TigerLilja.
Devotion Aura fades from Erebus.
Devotion Aura fades from Brynhilde.
Devotion Aura fades from BaleogFierce.

Damador
Dwarf Paladin
Level 8

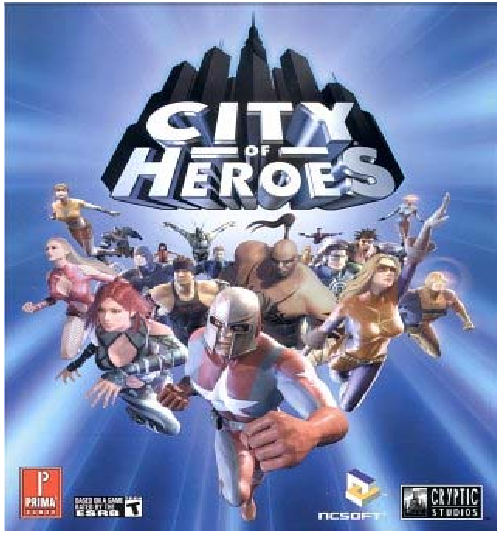
Disruptor: Online Persistent Environments

Disruptor: Online Persistent Environments

Disruptor: Online Persistent Environments

Disruptor: Online Persistent Environments

Traditional



Disruptor: Online Persistent Environments

Traditional

World of Warcraft
BusinessWeek
Virtual World, Real Money
She's fictional, lives inside an online game, but earns thousands of actual dollars there. And she's not alone.
BY ROBERT D. HOF (P. 72)

Anshe Chung

Ailin Graef

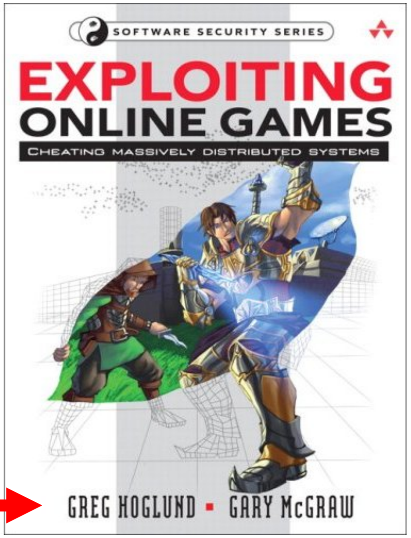
Not So Much

Disruptor: Online Persistent Environments

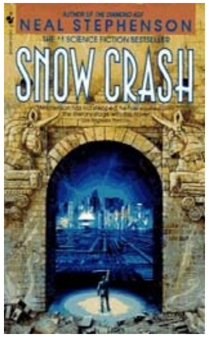
$1,000,000 Dollars US

Disruptor: Online Persistent Environments

$100,000 Dollars US

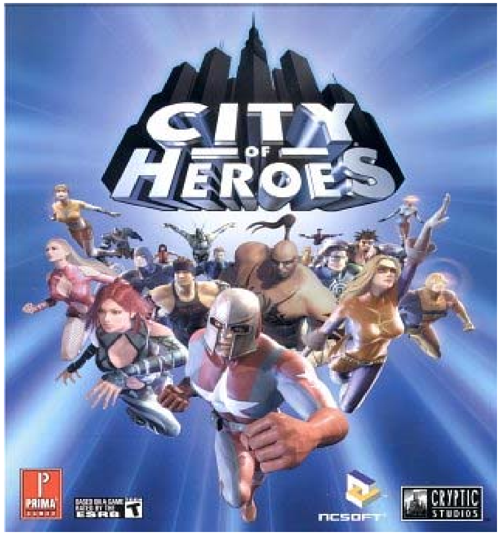

SOFTWARE SECURITY SERIES
EXPLOITING ONLINE GAMES
CHEATING MASSIVELY DISTRIBUTED SYSTEMS
GREG HOGLUND ▪ GARY McGRAW

Disruptor: Online Persistent Environments



Metaverse

1992



MMORPGs

Social in Nature

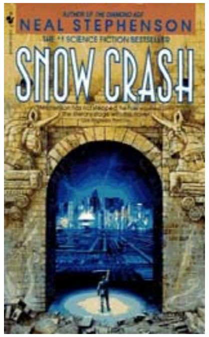
In-Game Email Clients

In-Game Chat

In-Game Applications to encourage group participation

Disruptor: Online Persistent Environments

myspace.com
a place for friends



Metaverse

1992

MMORPGs

Social in Nature

In-Game Email Clients

In-Game Chat

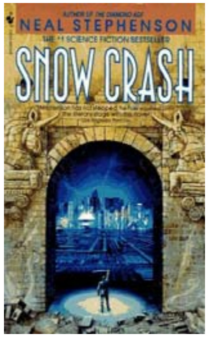
In-Game Applications to encourage group participation

IBM

Convergence

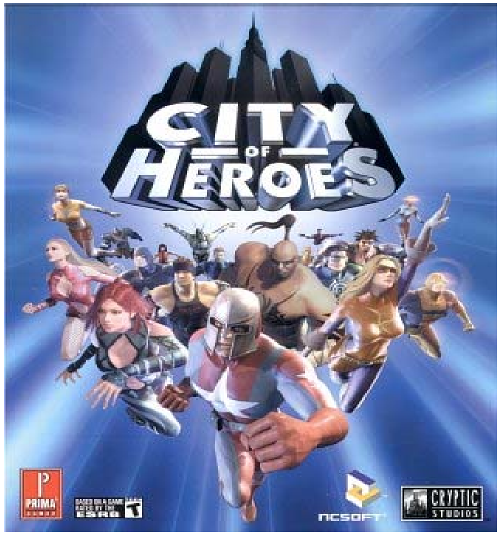
Disruptor: Online Persistent Environments

myspace.com
a place for friends



Metaverse

1992



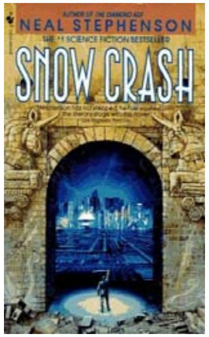
Convergence

IBM

SECOND LIFE

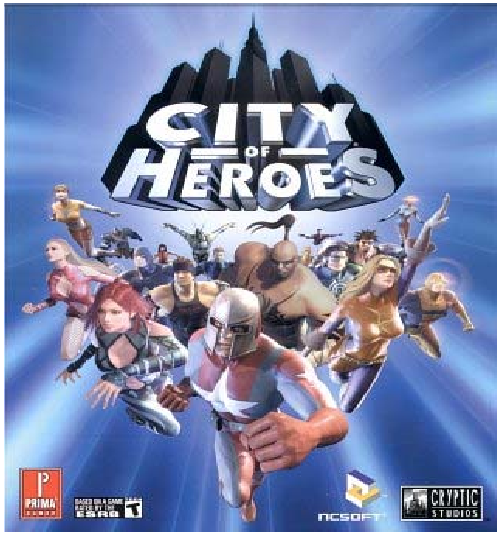
Disruptor: Online Persistent Environments

myspace.com
a place for friends



Metaverse

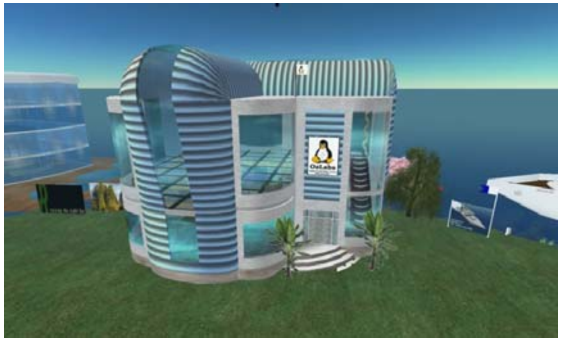
1992



Disruptor

Disruptor: Online Persistent Environments

Disruptor



Agenda

General Trends | Motivations | Innovation | Disruptors

VeriSign®

Q and A

Rick Howard

rhoward@verisign.com

VeriSign iDefense Security Intelligence Services

Where it all comes together.™