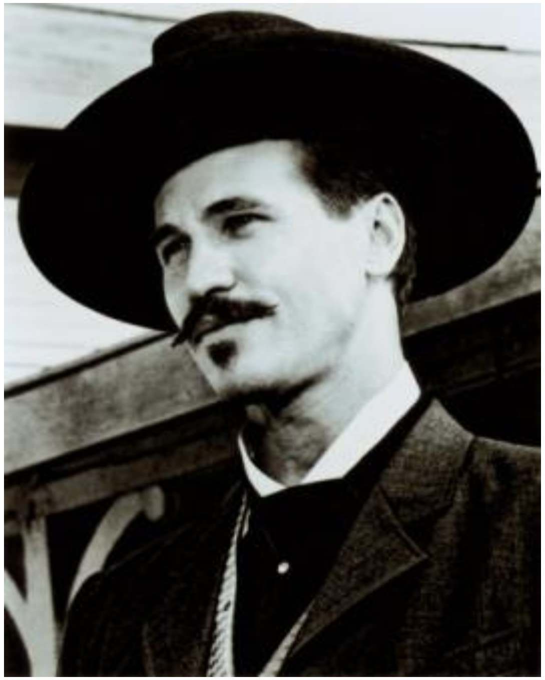
Why Black Hats Always Win

Val Smith (valsmith@attackresearch.com)
Chris (chris@sdnaconsulting.com)

Bios



Val Smith

- Affiliations:
  - Attack Research
  - Metasploit
- Work:
  - Attack Techniques Research
  - Pen Tester/ Exploit developer
  - Reverse Engineer
  - Malware Analyst

Previous Talks

- Exploiting malware & vm detection
- Kernel mode de-obfuscation of malware
- Data mining malware collections
- Tactical Exploitation
- Post Exploitation
- Analysis of foreign web attacks

Bios

Chris

Chris is a Security Consultant and Researcher with Secure DNA. Chris specializes in web based application development security. He has collaborated with some of the top security researchers and companies in the world and has performed static and dynamic security assessments for numerous companies and government agencies across the U.S. and Asia.

What are we talking about?

- Overview of:
  - White hat Methodologies
  - Black Hat Methodologies
- Attackers VS. Defenders
- Analysis of Black Hat techniques in the Wild
- Black Hat Methodologies Demystified
- How can this help you?
- What can you do?

Overview of White Hat Methodologies

Overview of White Hat Methodologies

- **Goals**
  - Focus on racking up numbers of hacked machines
  - Data to fill reports
  - Identifying mitigations
    - How to prevent the attack
  - Vulnerability footprint, not penetration
    - Often identifying accessible data is secondary goal

Overview of White Hat Methodologies

- **Goals**
  - No downtime for the customer
    - DoS usually not allowed
    - Even if it facilitates access via reboot, etc.
  - No modifications
    - Typically can't change:
      - Customer source code
      - Databases

  - Testing the response and detection mechanisms
    - Did the IDS catch us? Did they do anything?

Overview of White Hat Methodologies

- **Information Gathering**
  - Heavy focus on scans
    - Massive NMAPs / Nessus normal
  - Some overlap with Black Hat's
    - DNS / Domain lookup records
    - Google hacking
    - Personnel googling
  - Less concern for detection

Overview of White Hat Methodologies

- **Vulnerability Assessment**
  - – Almost always automated scanners
    - Detectable & fingerprintable
  - – Often a guess at potential vulnerability
  - – Focus on risk & threat analysis
    - Vulnerability Consequences
      - – How does this hurt client business
      - – Do they stand to lose money / customers?
      - – How likely is attack to occur

Overview of White Hat Methodologies

- **Exploitation**
  - Download and run exploits from milworm
    - Now defunct
    - How many pen test shops does this put out of business?
  - Securiteam & Security Focus
  - Core Impact / Canvas / Metasploit
  - Match up with nessus results
  - Usually no testing, run live against customer

Overview of White Hat Methodologies

- **Data Collection**
  - Screenshots
  - Sample documents
    - Just enough to prove access
  - No Analysis of attack paths
  - No prolonged infiltration
    - No long term sniffing / keylogging

Overview of Black Hat Methodologies

Overview of Black Hat Methodologies

- **Goals**
  - Wide ranging
  - Data, not just access focused
  - Targeting specific trusts
    - People weakest link in trust chains
  - Semi-unrelated access that may provide stepping stone
    - 6 degrees of separation
    - Any box on any network 6 degrees away from true target

Overview of Black Hat Methodologies

- **Goals**
  - Access to source
    - Let THEM do the hacking for you
      - They infect their own systems with backdoored updates
    - Source enables more assets
  - Example:
    - Target runs wordpress
    - Black Hat owns wordpress source server
    - Audit & Backdoor code
    - Surefire ownage of ultimate target in time

Overview of Black Hat Methodologies

- **Information Gathering**
  - Nothing is off limits
  - If needed info resides on un-related box its still in scope
  - Social networking
  - Call up target and ask for info
    - Call targets friends, co workers, family

Overview of Black Hat Methodologies

- **Vulnerability Assessment**
  - Attacker's often know what's vulnerable ahead of time
    - No need for noisy scans
  - More efficient method than white hat's trial & error
  - Stolen source code
    - Trojaned
    - Audited for 0days

Overview of Black Hat Methodologies

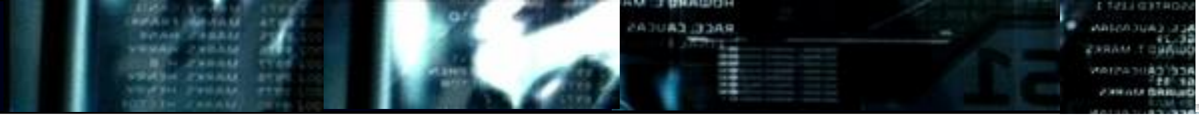
- **Vulnerability Assessment**
  - Non-traditional vulnerabilities
  - Example:
    - Software distro & licensing application
    - In house written by target
    - Installed on every computer
    - Runs with domain admin account privileges
    - Password changed every x min time interval
      - Accessible clear text in memory with debugger
    - Domain admin access to any machine for x minutes

Overview of Black Hat Methodologies

- **Exploitation**
  - 0 Days
    - Often only used when public bugs don't work
    - Avoid risking burning unpublished bug if possible
  - Usually interception from another box is better
  - Ex. Metasploit usually waits for 0day to become public before trunking
  - Wait till bug becomes 1day then blend in with worm traffic

Overview of Black Hat Methodologies

- **Data Targets**
  - Mail spools
  - Backup files
  - Database dumps
  - Sniffer logs
  - Keystrokes and chat logs
  - Access tokens
    - Crypto keys, kerberos tickets, windows domain tokens
  - Targets of opportunity
    - Maybe data *xyz* is the goal but *abc* is found more valuable



Overview of Black Hat Methodologies

- **Data Theft**
  - Client Injection / Exploitation
    - Vulnerable Client Applications
      - BSD IRC client exploit
    - Browsers
      - Grab sensitive data in browser POST
        - » Before its SSL encrypted on screen keyboards = useless
  - Backdoors
    - Access Points
    - Services
    - Utilities

Attackers vs. Defenders

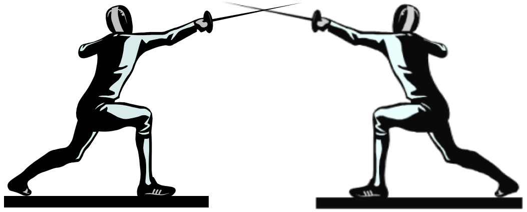
Attackers vs. Defenders

- **Defenders**:
  - Limited resources
  - Limited time
  - Rules of engagement
  - Consequences based on performance
    - If a pen tester never gets in, they stop getting hired
  - Motivation
- **Attackers:**
  - Unlimited resources
  - Unlimited time
  - On a long enough timeline everything gets owned
  - If attacker targets you, odds of success increase over time
  - No consequences to not getting in
  - Little to no rules
  - Motivation

Attackers vs. Defenders

- White Hats usually assigned limited block of IP addresses
- Unable to go beyond the scope of approved list

- Black Hats usually know one piece of information and have to expand from there
  - Domain Name
  - Email address



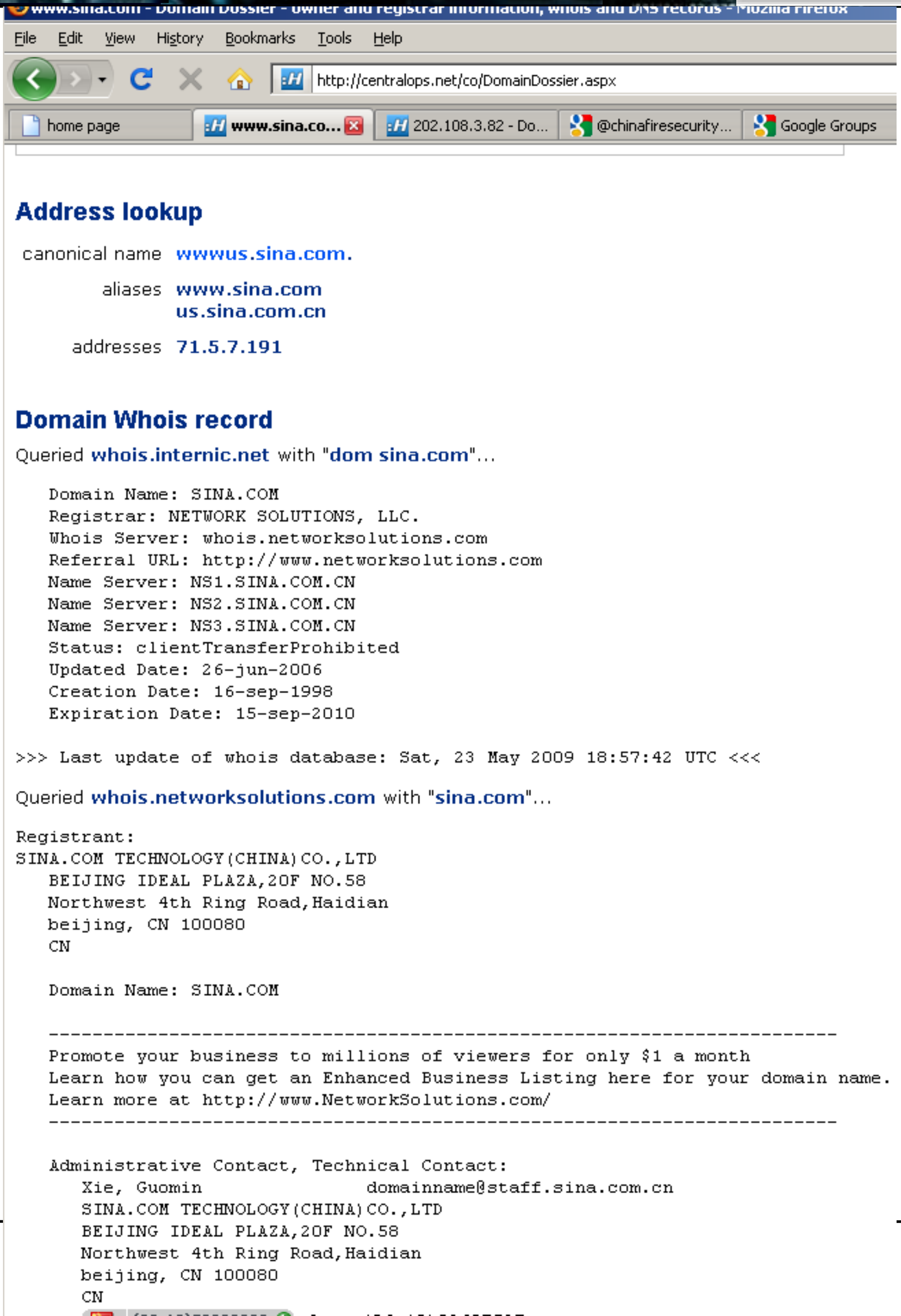
Attackers vs. Defenders

- Black Hats need techniques for discovering target related IPs and client side info
  - News group mail header harvesting
  - Proxy log analysis site mining
  - Backscatter spam
  - Botsvsbrowsers

You know the target’s domain name

Look at the IP range

Unlikely to be the target’s operational LAN


www.sina.com - Domain Dossier - owner and registrar information, whois and DNS records - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://centralops.net/co/DomainDossier.aspx
home page
www.sina.co...
202.108.3.82 - Do...
@chinafiresecurity...
Google Groups

Address lookup

canonical name wwwus.sina.com.

aliases www.sina.com
us.sina.com.cn

addresses 71.5.7.191

Domain Whois record

Queried whois.internic.net with "dom sina.com"...

```
   Domain Name: SINA.COM
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com
   Name Server: NS1.SINA.COM.CN
   Name Server: NS2.SINA.COM.CN
   Name Server: NS3.SINA.COM.CN
   Status: clientTransferProhibited
   Updated Date: 26-jun-2006
   Creation Date: 16-sep-1998
   Expiration Date: 15-sep-2010

>>> Last update of whois database: Sat, 23 May 2009 18:57:42 UTC <<<
```

Queried whois.networksolutions.com with "sina.com"...

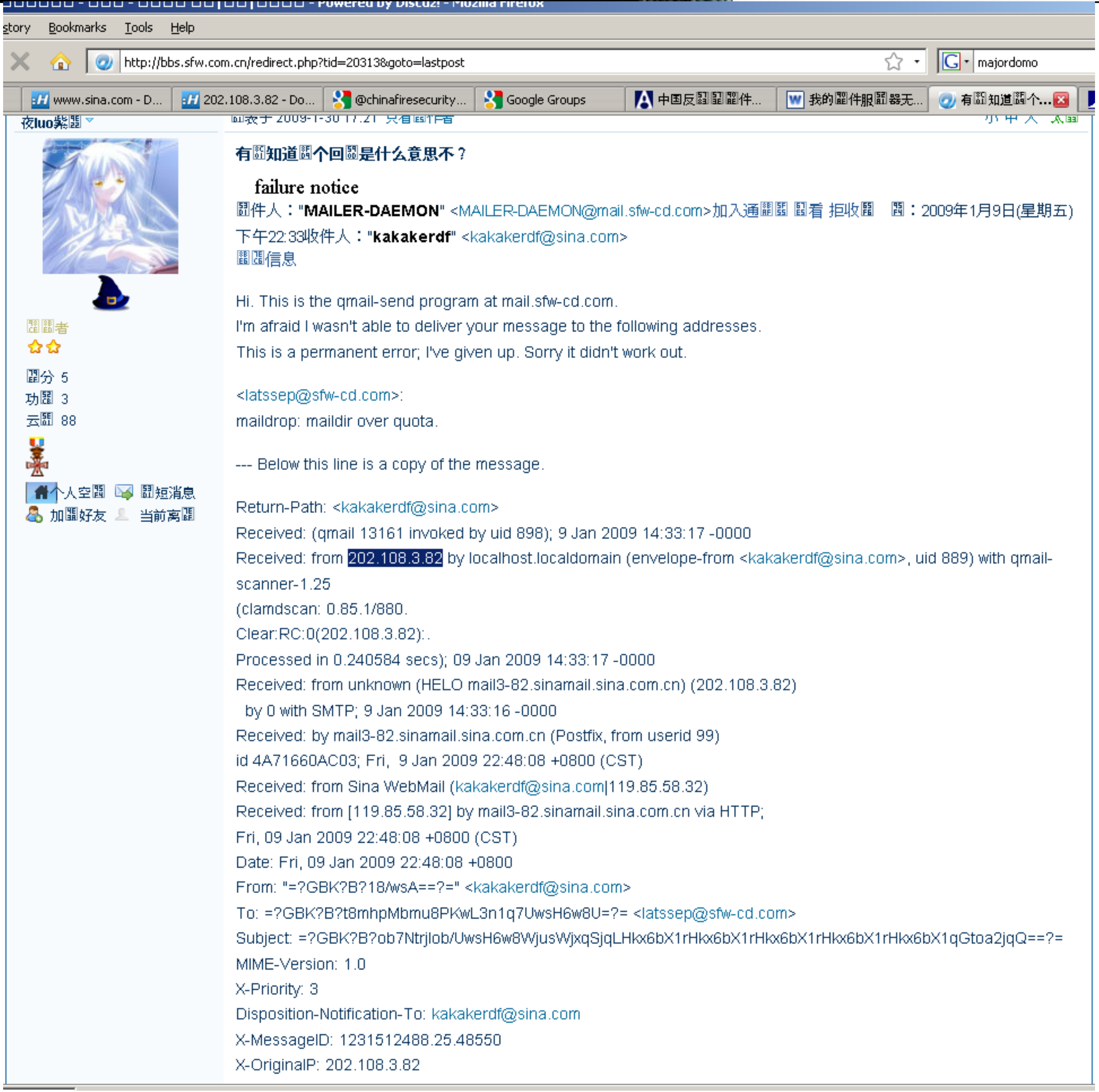
```
Registrant:
SINA.COM TECHNOLOGY(CHINA)CO.,LTD
   BEIJING IDEAL PLAZA,20F NO.58
   Northwest 4th Ring Road,Haidian
   beijing, CN 100080
   CN

   Domain Name: SINA.COM

   ------------------------------------------------------------------------
   Promote your business to millions of viewers for only $1 a month
   Learn how you can get an Enhanced Business Listing here for your domain name.
   Learn more at http://www.NetworkSolutions.com/
   ------------------------------------------------------------------------

   Administrative Contact, Technical Contact:
      Xie, Guomin              domainname@staff.sina.com.cn
      SINA.COM TECHNOLOGY(CHINA)CO.,LTD
      BEIJING IDEAL PLAZA,20F NO.58
      Northwest 4th Ring Road,Haidian
      beijing, CN 100080
      CN
```

Searching newsgroup postings for the target domain yields an email bounce with headers

Header shows the IP the email was sent from

Likely to be the target LAN or a home IP of a user on the target LAN (vpn maybe?)

Sometimes the headers in mailing list posts themselves have the same info



http://bbs.sfw.com.cn/redirect.php?tid=20313&goto=lastpost

夜luo紫□

□□者

□分 5
功□ 3
云□ 88

有□知道□个回□是什么意思不？

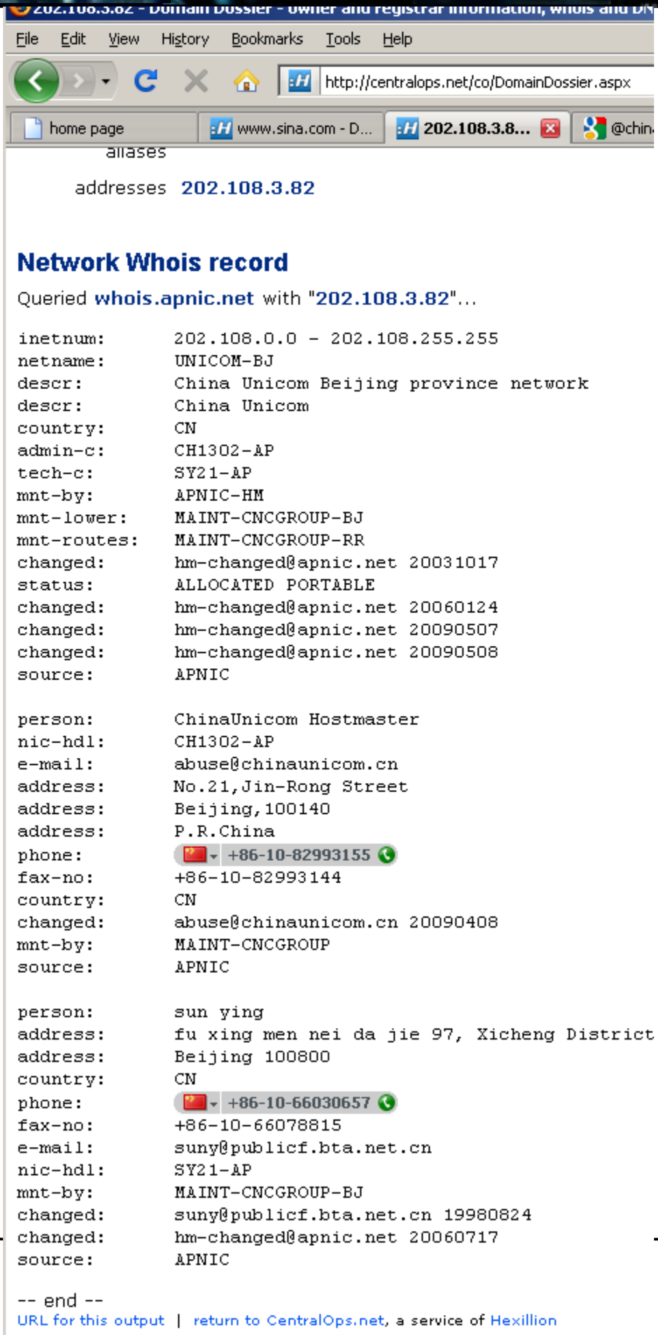
failure notice

□件人："MAILER-DAEMON" <MAILER-DAEMON@mail.sfw-cd.com>加入通□□ □看 拒收□ □：2009年1月9日(星期五)下午22:33收件人："kakakerdf" <kakakerdf@sina.com>
□□信息

```
Hi. This is the qmail-send program at mail.sfw-cd.com.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<latssep@sfw-cd.com>:
maildrop: maildir over quota.

--- Below this line is a copy of the message.

Return-Path: <kakakerdf@sina.com>
Received: (qmail 13161 invoked by uid 898); 9 Jan 2009 14:33:17 -0000
Received: from 202.108.3.82 by localhost.localdomain (envelope-from <kakakerdf@sina.com>, uid 889) with qmail-
scanner-1.25
(clamdscan: 0.85.1/880.
Clear:RC:0(202.108.3.82):.
Processed in 0.240584 secs); 09 Jan 2009 14:33:17 -0000
Received: from unknown (HELO mail3-82.sinamail.sina.com.cn) (202.108.3.82)
 by 0 with SMTP; 9 Jan 2009 14:33:16 -0000
Received: by mail3-82.sinamail.sina.com.cn (Postfix, from userid 99)
id 4A71660AC03; Fri,  9 Jan 2009 22:48:08 +0800 (CST)
Received: from Sina WebMail (kakakerdf@sina.com|119.85.58.32)
Received: from [119.85.58.32] by mail3-82.sinamail.sina.com.cn via HTTP;
Fri, 09 Jan 2009 22:48:08 +0800 (CST)
Date: Fri, 09 Jan 2009 22:48:08 +0800
From: "=?GBK?B?18/wsA==?=" <kakakerdf@sina.com>
To: =?GBK?B?t8mhpMbmu8PKwL3n1q7UwsH6w8U=?= <latssep@sfw-cd.com>
Subject: =?GBK?B?ob7Ntrjlob/UwsH6w8WjusWjxqSjqLHkx6bX1rHkx6bX1rHkx6bX1rHkx6bX1rHkx6bX1qGtoa2jqQ==?=
MIME-Version: 1.0
X-Priority: 3
Disposition-Notification-To: kakakerdf@sina.com
X-MessageID: 1231512488.25.48550
X-OriginalP: 202.108.3.82
```

Check the IP the email came from

Totally different network, in the target country


202.108.3.82 - Domain Dossier - owner and registrar information, whois and DN
File Edit View History Bookmarks Tools Help
http://centralops.net/co/DomainDossier.aspx
home page
www.sina.com - D...
202.108.3.8...
@chin

```
aliases

addresses  202.108.3.82
```

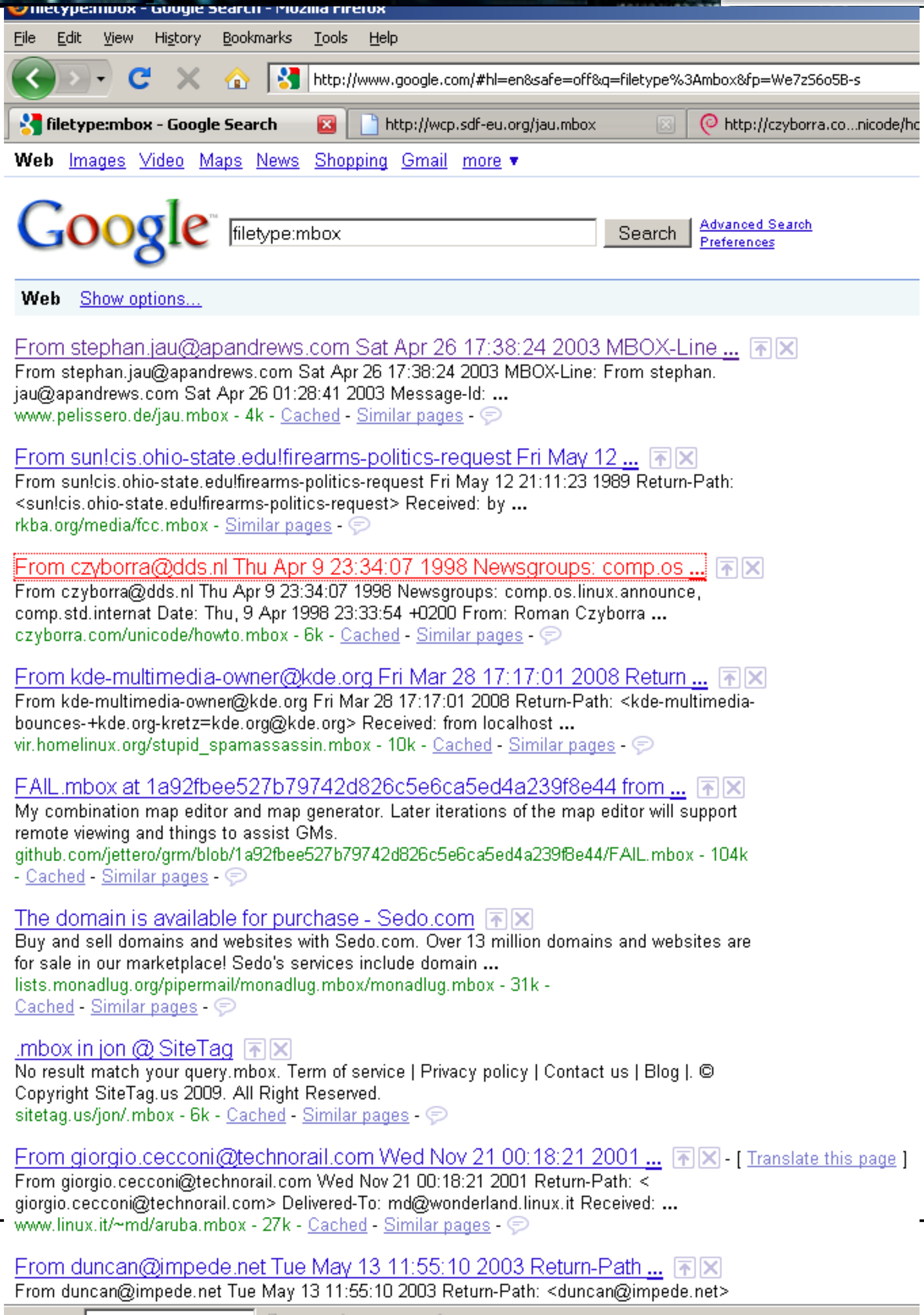
Network Whois record

Queried **whois.apnic.net** with "**202.108.3.82**"...

```
inetnum:       202.108.0.0 - 202.108.255.255
netname:       UNICOM-BJ
descr:         China Unicom Beijing province network
descr:         China Unicom
country:       CN
admin-c:       CH1302-AP
tech-c:        SY21-AP
mnt-by:        APNIC-HM
mnt-lower:     MAINT-CNCGROUP-BJ
mnt-routes:    MAINT-CNCGROUP-RR
changed:       hm-changed@apnic.net 20031017
status:        ALLOCATED PORTABLE
changed:       hm-changed@apnic.net 20060124
changed:       hm-changed@apnic.net 20090507
changed:       hm-changed@apnic.net 20090508
source:        APNIC

person:        ChinaUnicom Hostmaster
nic-hdl:       CH1302-AP
e-mail:        abuse@chinaunicom.cn
address:       No.21,Jin-Rong Street
address:       Beijing,100140
address:       P.R.China
phone:         +86-10-82993155
fax-no:        +86-10-82993144
country:       CN
changed:       abuse@chinaunicom.cn 20090408
mnt-by:        MAINT-CNCGROUP
source:        APNIC

person:        sun ying
address:       fu xing men nei da jie 97, Xicheng District
address:       Beijing 100800
country:       CN
phone:         +86-10-66030657
fax-no:        +86-10-66078815
e-mail:        suny@publicf.bta.net.cn
nic-hdl:       SY21-AP
mnt-by:        MAINT-CNCGROUP-BJ
changed:       suny@publicf.bta.net.cn 19980824
changed:       hm-changed@apnic.net 20060717
source:        APNIC

-- end --
```

URL for this output | return to CentralOps.net, a service of Hexillion

Search for file types associated with mail boxes to gather client side information


filetype:mbox - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/#hl=en&safe=off&q=filetype%3Ambox&fp=We7zS6o5B-s
filetype:mbox - Google Search
http://wcp.sdf-eu.org/jau.mbox
http://czyborra.co...nicode/hc
Web Images Video Maps News Shopping Gmail more ▾
Google
Search
Advanced Search
Preferences
Web Show options...

filetype:mbox

From stephan.jau@apandrews.com Sat Apr 26 17:38:24 2003 MBOX-Line ...
From stephan.jau@apandrews.com Sat Apr 26 17:38:24 2003 MBOX-Line: From stephan.jau@apandrews.com Sat Apr 26 01:28:41 2003 Message-Id: ...
www.pelissero.de/jau.mbox - 4k - Cached - Similar pages -

From sun!cis.ohio-state.edu!firearms-politics-request Fri May 12 ...
From sun!cis.ohio-state.edu!firearms-politics-request Fri May 12 21:11:23 1989 Return-Path: <sun!cis.ohio-state.edu!firearms-politics-request> Received: by ...
rkba.org/media/fcc.mbox - Similar pages -

From czyborra@dds.nl Thu Apr 9 23:34:07 1998 Newsgroups: comp.os ...
From czyborra@dds.nl Thu Apr 9 23:34:07 1998 Newsgroups: comp.os.linux.announce, comp.std.internat Date: Thu, 9 Apr 1998 23:33:54 +0200 From: Roman Czyborra ...
czyborra.com/unicode/howto.mbox - 6k - Cached - Similar pages -

From kde-multimedia-owner@kde.org Fri Mar 28 17:17:01 2008 Return ...
From kde-multimedia-owner@kde.org Fri Mar 28 17:17:01 2008 Return-Path: <kde-multimedia-bounces-+kde.org-kretz=kde.org@kde.org> Received: from localhost ...
vir.homelinux.org/stupid_spamassassin.mbox - 10k - Cached - Similar pages -

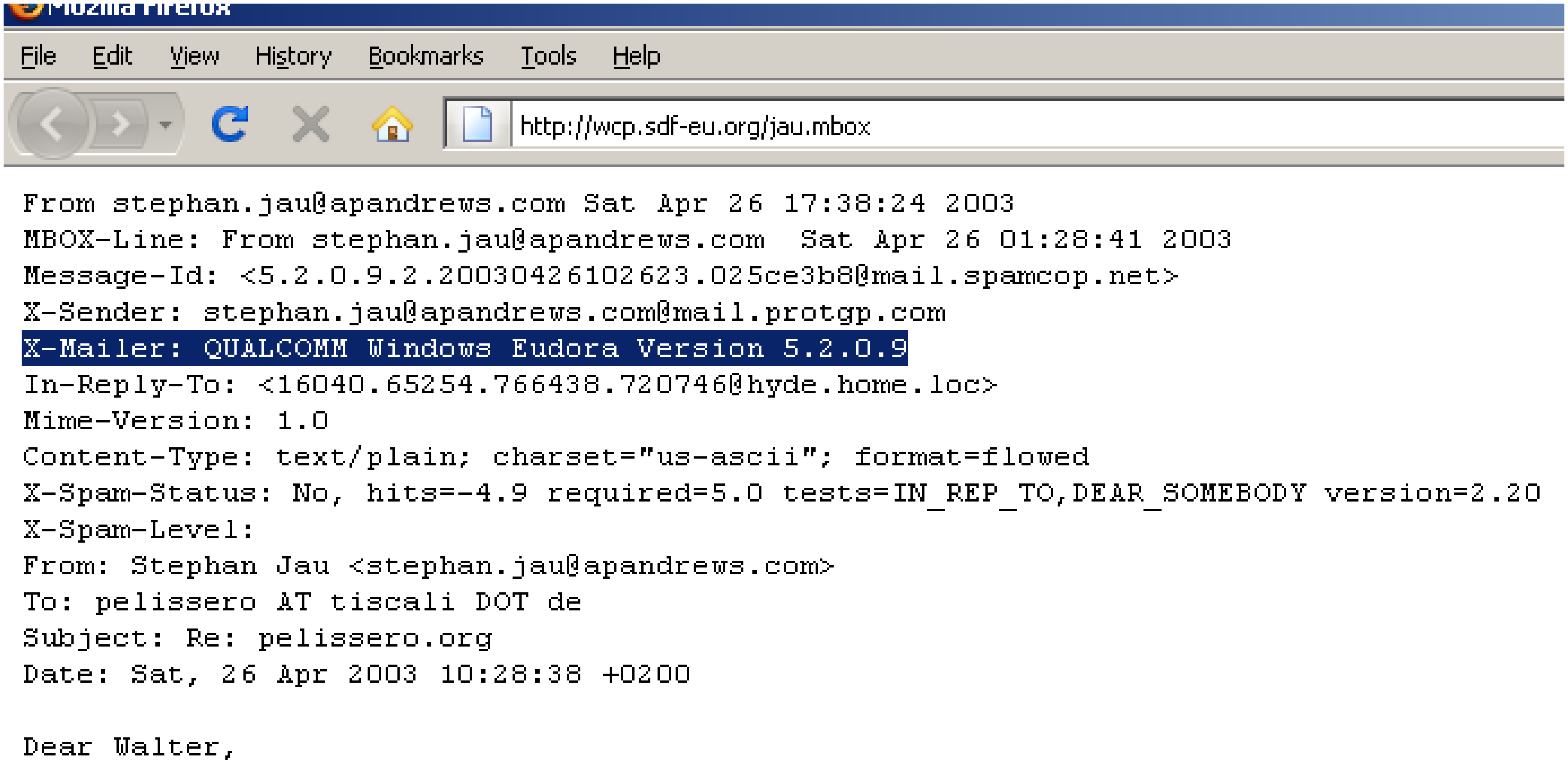
FAIL.mbox at 1a92fbee527b79742d826c5e6ca5ed4a239f8e44 from ...
My combination map editor and map generator. Later iterations of the map editor will support remote viewing and things to assist GMs.
github.com/jettero/grm/blob/1a92fbee527b79742d826c5e6ca5ed4a239f8e44/FAIL.mbox - 104k - Cached - Similar pages -

The domain is available for purchase - Sedo.com
Buy and sell domains and websites with Sedo.com. Over 13 million domains and websites are for sale in our marketplace! Sedo's services include domain ...
lists.monadlug.org/pipermail/monadlug.mbox/monadlug.mbox - 31k - Cached - Similar pages -

.mbox in jon @ SiteTag
No result match your query.mbox. Term of service | Privacy policy | Contact us | Blog |. © Copyright SiteTag.us 2009. All Right Reserved.
sitetag.us/jon/.mbox - 6k - Cached - Similar pages -

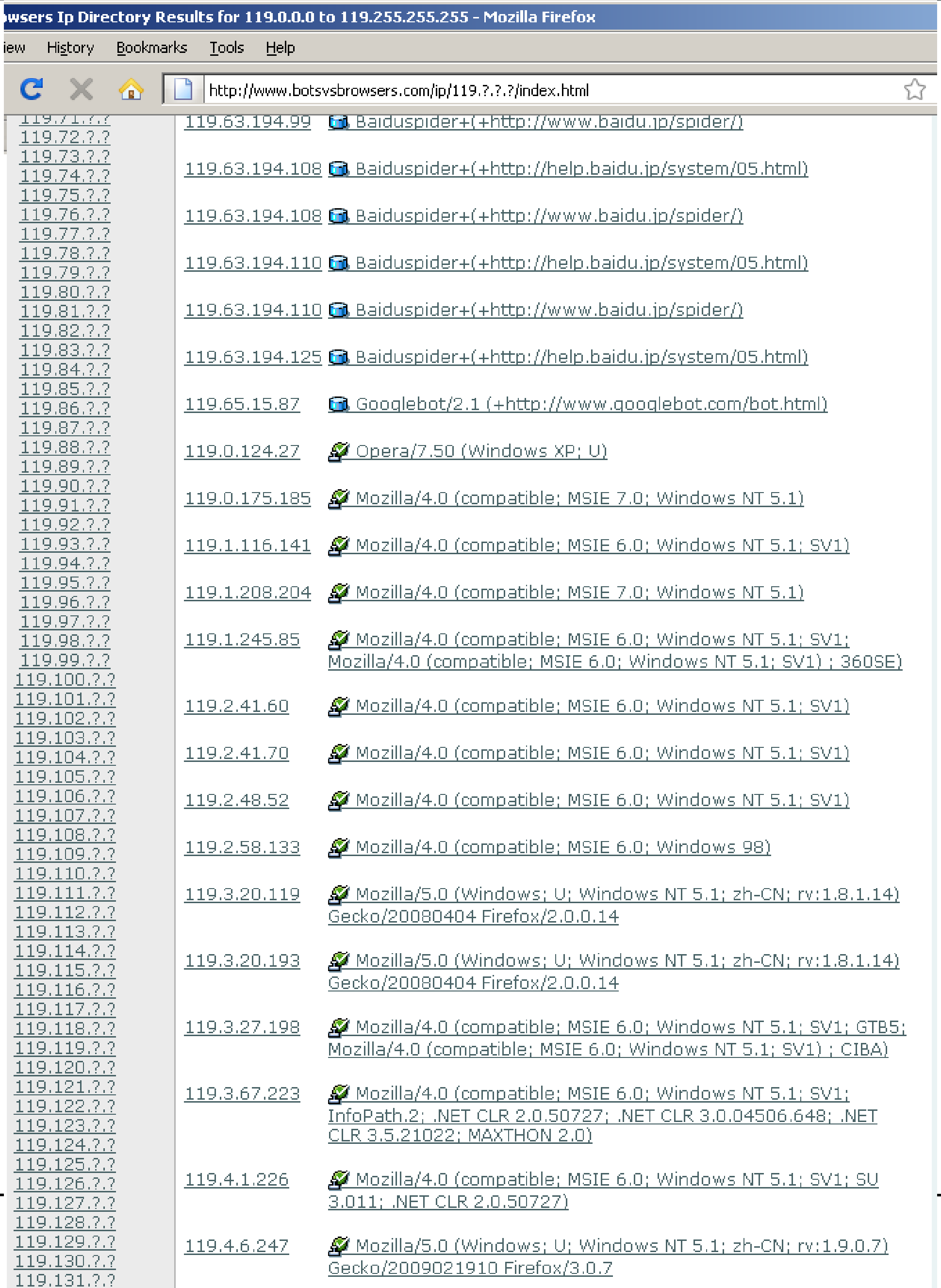
From giorgio.cecconi@technorail.com Wed Nov 21 00:18:21 2001 ... - [Translate this page]
From giorgio.cecconi@technorail.com Wed Nov 21 00:18:21 2001 Return-Path: < giorgio.cecconi@technorail.com> Delivered-To: md@wonderland.linux.it Received: ...
www.linux.it/~md/aruba.mbox - 27k - Cached - Similar pages -

From duncan@impede.net Tue May 13 11:55:10 2003 Return-Path ...
From duncan@impede.net Tue May 13 11:55:10 2003 Return-Path: <duncan@impede.net>



```
From stephan.jau@apandrews.com Sat Apr 26 17:38:24 2003
MBOX-Line: From stephan.jau@apandrews.com  Sat Apr 26 01:28:41 2003
Message-Id: <5.2.0.9.2.20030426102623.025ce3b8@mail.spamcop.net>
X-Sender: stephan.jau@apandrews.com@mail.protgp.com
X-Mailer: QUALCOMM Windows Eudora Version 5.2.0.9
In-Reply-To: <16040.65254.766438.720746@hyde.home.loc>
Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; format=flowed
X-Spam-Status: No, hits=-4.9 required=5.0 tests=IN_REP_TO,DEAR_SOMEBODY version=2.20
X-Spam-Level:
From: Stephan Jau <stephan.jau@apandrews.com>
To: pelissero AT tiscali DOT de
Subject: Re: pelissero.org
Date: Sat, 26 Apr 2003 10:28:38 +0200

Dear Walter,
```

Botsvsbrowsers gives you by IP address client information such as browser and operating system



wsers Ip Directory Results for 119.0.0.0 to 119.255.255.255 - Mozilla Firefox

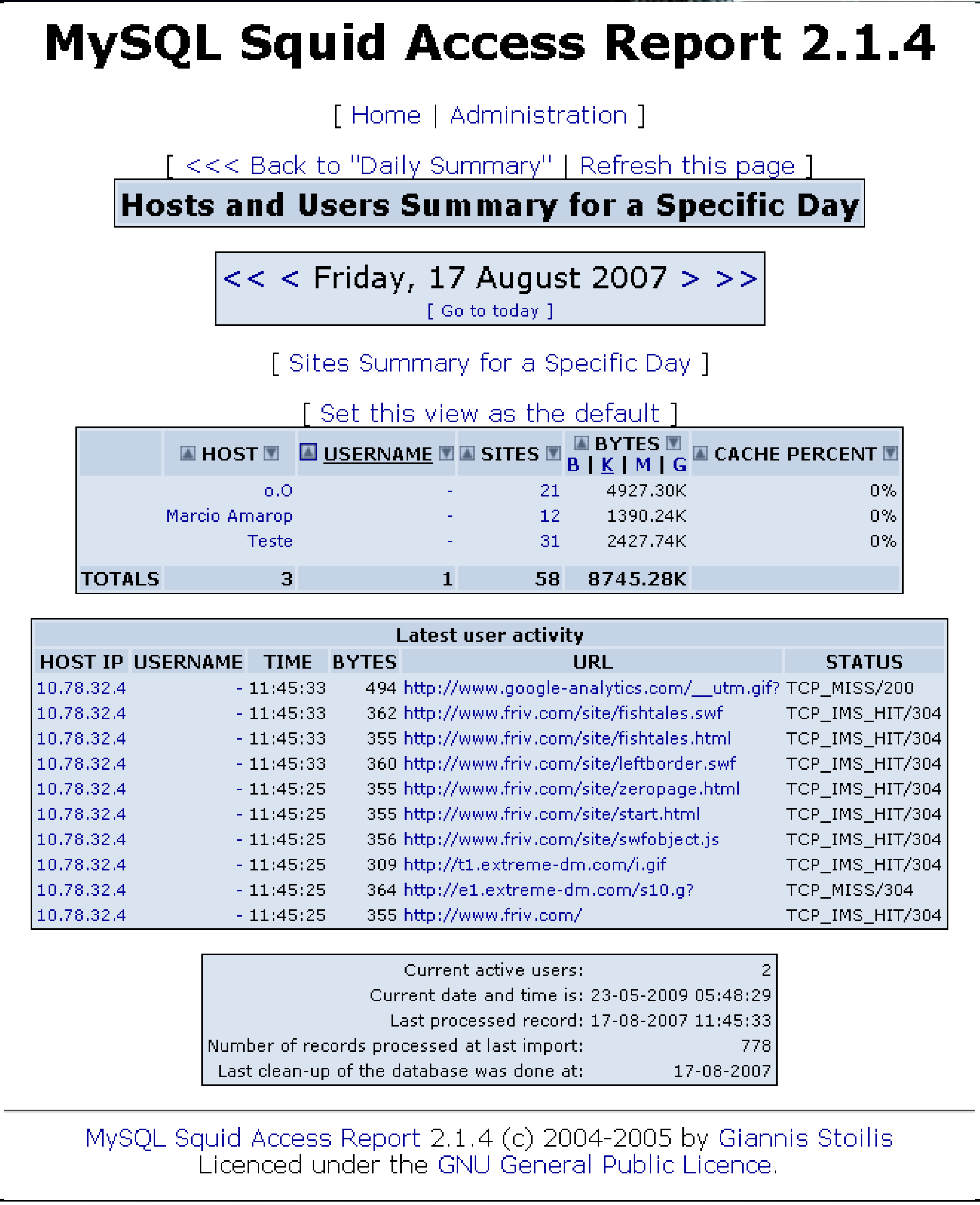
http://www.botsvsbrowsers.com/ip/119.?.?.?/index.html

119.71.?.?
119.72.?.?
119.73.?.?
119.74.?.?
119.75.?.?
119.76.?.?
119.77.?.?
119.78.?.?
119.79.?.?
119.80.?.?
119.81.?.?
119.82.?.?
119.83.?.?
119.84.?.?
119.85.?.?
119.86.?.?
119.87.?.?
119.88.?.?
119.89.?.?
119.90.?.?
119.91.?.?
119.92.?.?
119.93.?.?
119.94.?.?
119.95.?.?
119.96.?.?
119.97.?.?
119.98.?.?
119.99.?.?
119.100.?.?
119.101.?.?
119.102.?.?
119.103.?.?
119.104.?.?
119.105.?.?
119.106.?.?
119.107.?.?
119.108.?.?
119.109.?.?
119.110.?.?
119.111.?.?
119.112.?.?
119.113.?.?
119.114.?.?
119.115.?.?
119.116.?.?
119.117.?.?
119.118.?.?
119.119.?.?
119.120.?.?
119.121.?.?
119.122.?.?
119.123.?.?
119.124.?.?
119.125.?.?
119.126.?.?
119.127.?.?
119.128.?.?
119.129.?.?
119.130.?.?
119.131.?.?

119.63.194.99	Baiduspider+(+http://www.baidu.jp/spider/)
119.63.194.108	Baiduspider+(+http://help.baidu.jp/system/05.html)
119.63.194.108	Baiduspider+(+http://www.baidu.jp/spider/)
119.63.194.110	Baiduspider+(+http://help.baidu.jp/system/05.html)
119.63.194.110	Baiduspider+(+http://www.baidu.jp/spider/)
119.63.194.125	Baiduspider+(+http://help.baidu.jp/system/05.html)
119.65.15.87	Googlebot/2.1 (+http://www.googlebot.com/bot.html)
119.0.124.27	Opera/7.50 (Windows XP; U)
119.0.175.185	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
119.1.116.141	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.1.208.204	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
119.1.245.85	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; 360SE)
119.2.41.60	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.2.41.70	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.2.48.52	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.2.58.133	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
119.3.20.119	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14
119.3.20.193	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14
119.3.27.198	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB5; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; CIBA)
119.3.67.223	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; MAXTHON 2.0)
119.4.1.226	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; SU 3.011; .NET CLR 2.0.50727)
119.4.6.247	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7

Some sites have exposed squid proxy log analysis pages

In this view you can see some hostnames and internal IP addresses



MySQL Squid Access Report 2.1.4

[Home | Administration]

[<<< Back to "Daily Summary" | Refresh this page]

Hosts and Users Summary for a Specific Day

<< < Friday, 17 August 2007 > >>
[Go to today]

[Sites Summary for a Specific Day]

[Set this view as the default]

	HOST	USERNAME	SITES	BYTES B | K | M | G	CACHE PERCENT
	o.O	-	21	4927.30K	0%
	Marcio Amarop	-	12	1390.24K	0%
	Teste	-	31	2427.74K	0%
TOTALS	3	1	58	8745.28K	

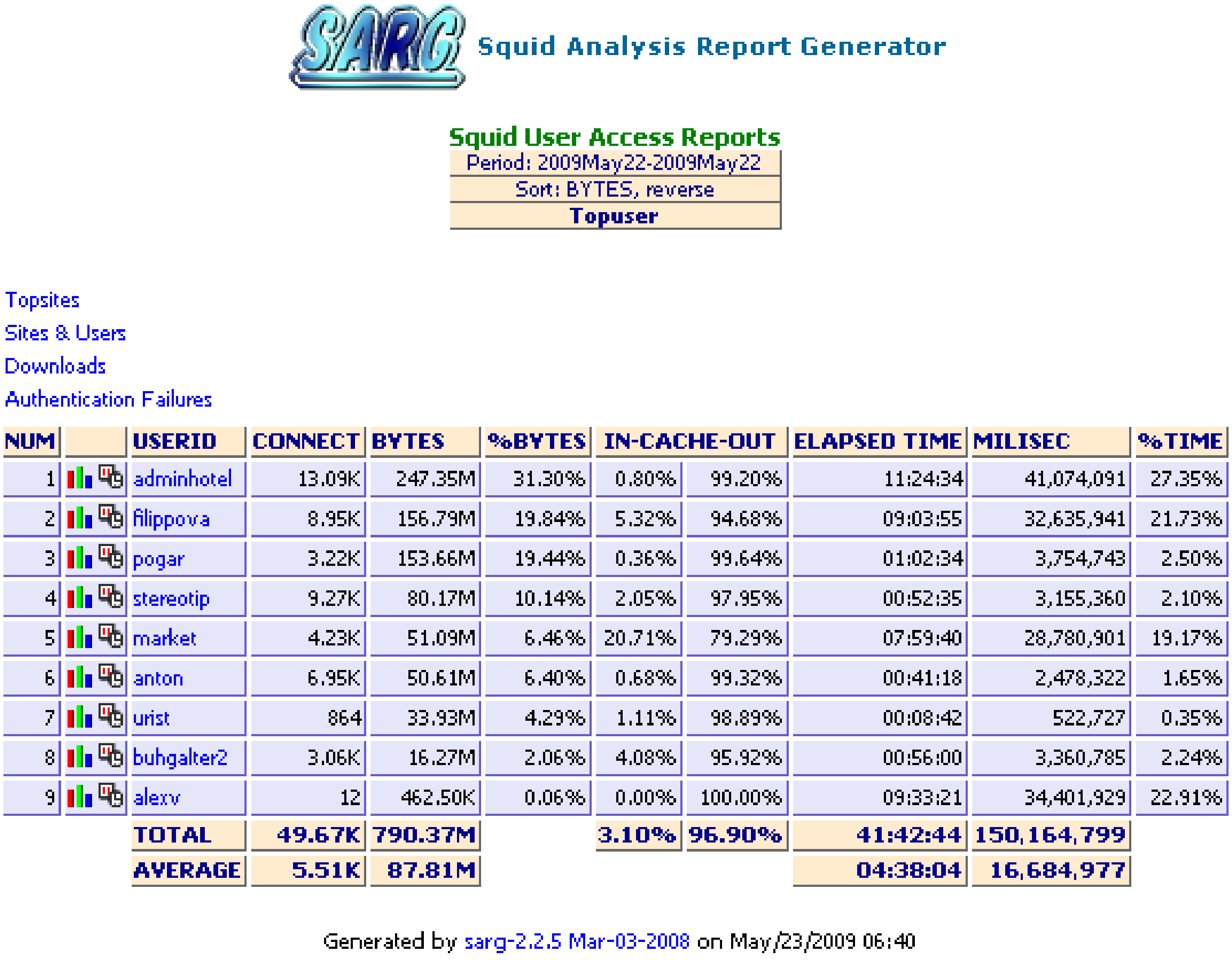
Latest user activity

HOST IP	USERNAME	TIME	BYTES	URL	STATUS
10.78.32.4	-	11:45:33	494	http://www.google-analytics.com/__utm.gif?	TCP_MISS/200
10.78.32.4	-	11:45:33	362	http://www.friv.com/site/fishtales.swf	TCP_IMS_HIT/304
10.78.32.4	-	11:45:33	355	http://www.friv.com/site/fishtales.html	TCP_IMS_HIT/304
10.78.32.4	-	11:45:33	360	http://www.friv.com/site/leftborder.swf	TCP_IMS_HIT/304
10.78.32.4	-	11:45:25	355	http://www.friv.com/site/zeropage.html	TCP_IMS_HIT/304
10.78.32.4	-	11:45:25	355	http://www.friv.com/site/start.html	TCP_IMS_HIT/304
10.78.32.4	-	11:45:25	356	http://www.friv.com/site/swfobject.js	TCP_IMS_HIT/304
10.78.32.4	-	11:45:25	309	http://t1.extreme-dm.com/i.gif	TCP_IMS_HIT/304
10.78.32.4	-	11:45:25	364	http://e1.extreme-dm.com/s10.g?	TCP_MISS/304
10.78.32.4	-	11:45:25	355	http://www.friv.com/	TCP_IMS_HIT/304

Current active users:	2
Current date and time is:	23-05-2009 05:48:29
Last processed record:	17-08-2007 11:45:33
Number of records processed at last import:	778
Last clean-up of the database was done at:	17-08-2007

MySQL Squid Access Report 2.1.4 (c) 2004-2005 by Giannis Stoilis
Licenced under the GNU General Public Licence.

This view shows userIDs and traffic quantities



SARG Squid Analysis Report Generator

Squid User Access Reports

Period: 2009May22-2009May22

Sort: BYTES, reverse

Topuser

Topsites

Sites & Users

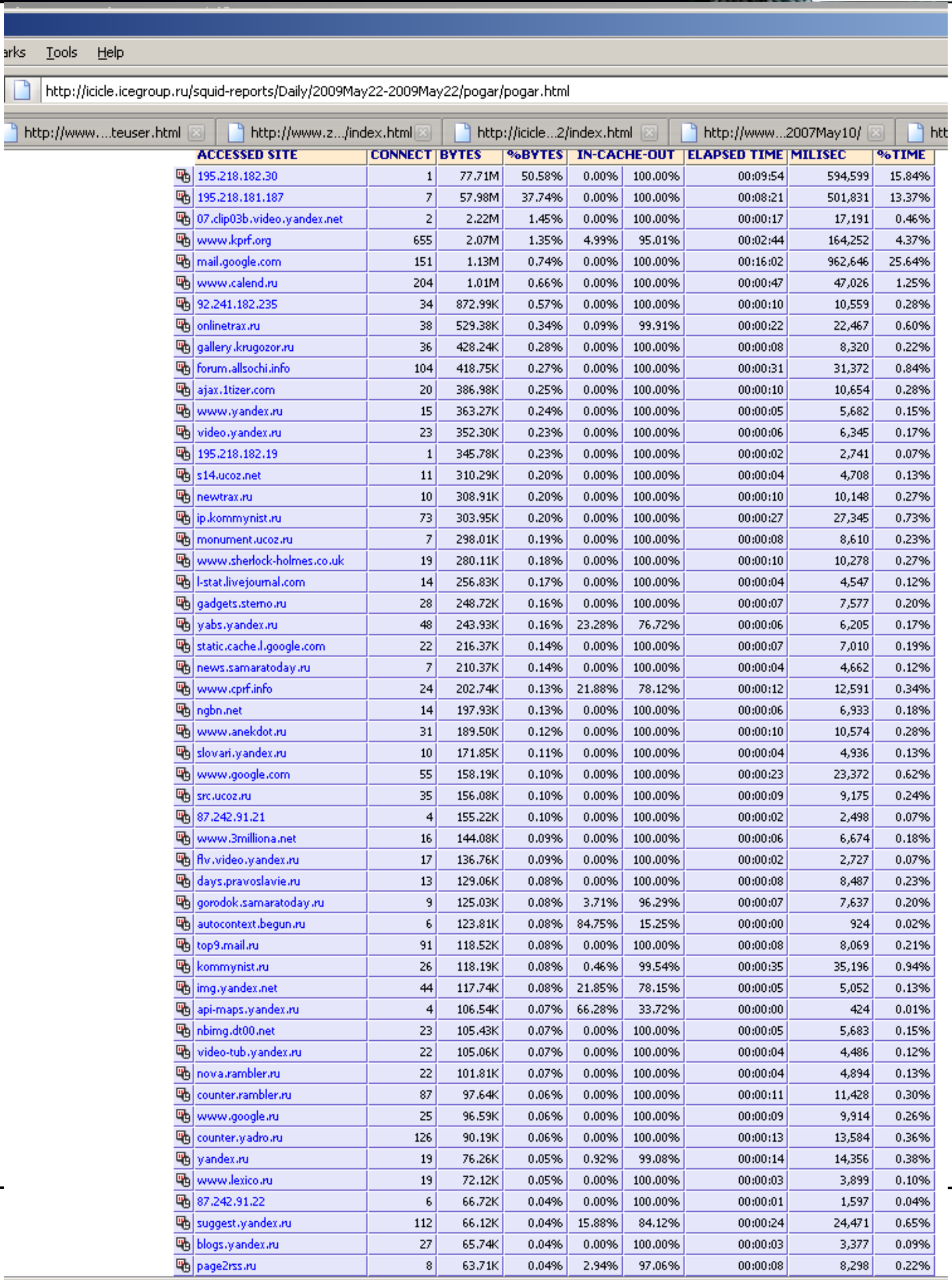
Downloads

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1		adminhotel	13.09K	247.35M	31.30%	0.80%	99.20%	11:24:34	41,074,091	27.35%
2		filippova	8.95K	156.79M	19.84%	5.32%	94.68%	09:03:55	32,635,941	21.73%
3		pogar	3.22K	153.66M	19.44%	0.36%	99.64%	01:02:34	3,754,743	2.50%
4		stereotip	9.27K	80.17M	10.14%	2.05%	97.95%	00:52:35	3,155,360	2.10%
5		market	4.23K	51.09M	6.46%	20.71%	79.29%	07:59:40	28,780,901	19.17%
6		anton	6.95K	50.61M	6.40%	0.68%	99.32%	00:41:18	2,478,322	1.65%
7		urist	864	33.93M	4.29%	1.11%	98.89%	00:08:42	522,727	0.35%
8		buhgalter2	3.06K	16.27M	2.06%	4.08%	95.92%	00:56:00	3,360,785	2.24%
9		alexv	12	462.50K	0.06%	0.00%	100.00%	09:33:21	34,401,929	22.91%
		TOTAL	**49.67K**	**790.37M**		**3.10%**	**96.90%**	**41:42:44**	**150,164,799**	
		AVERAGE	**5.51K**	**87.81M**				**04:38:04**	**16,684,977**	

Generated by sarg-2.2.5 Mar-03-2008 on May/23/2009 06:40

This view shows addresses a particular user is browsing to

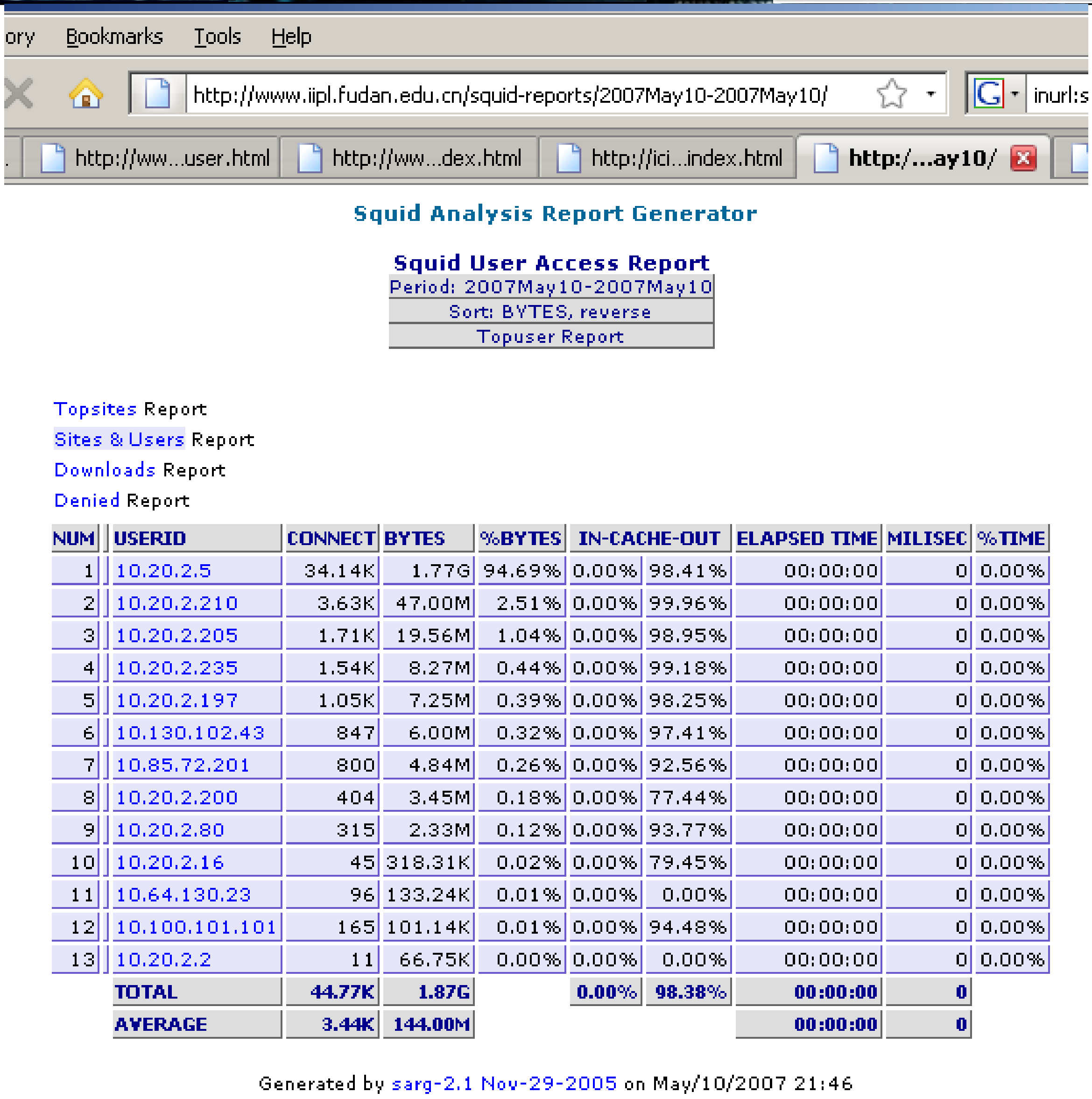


arks
Tools
Help
http://www....teuser.html
http://www.z.../index.html
http://icicle...2/index.html
http://www...2007May10/
htt

http://icicle.icegroup.ru/squid-reports/Daily/2009May22-2009May22/pogar/pogar.html

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
195.218.182.30	1	77.71M	50.58%	0.00%	100.00%	00:09:54	594,599	15.84%
195.218.181.187	7	57.98M	37.74%	0.00%	100.00%	00:08:21	501,831	13.37%
07.clip03b.video.yandex.net	2	2.22M	1.45%	0.00%	100.00%	00:00:17	17,191	0.46%
www.kprf.org	655	2.07M	1.35%	4.99%	95.01%	00:02:44	164,252	4.37%
mail.google.com	151	1.13M	0.74%	0.00%	100.00%	00:16:02	962,646	25.64%
www.calend.ru	204	1.01M	0.66%	0.00%	100.00%	00:00:47	47,026	1.25%
92.241.182.235	34	872.99K	0.57%	0.00%	100.00%	00:00:10	10,559	0.28%
onlinetrax.ru	38	529.38K	0.34%	0.09%	99.91%	00:00:22	22,467	0.60%
gallery.krugozor.ru	36	428.24K	0.28%	0.00%	100.00%	00:00:08	8,320	0.22%
forum.allsochi.info	104	418.75K	0.27%	0.00%	100.00%	00:00:31	31,372	0.84%
ajax.1tizer.com	20	386.98K	0.25%	0.00%	100.00%	00:00:10	10,654	0.28%
www.yandex.ru	15	363.27K	0.24%	0.00%	100.00%	00:00:05	5,682	0.15%
video.yandex.ru	23	352.30K	0.23%	0.00%	100.00%	00:00:06	6,345	0.17%
195.218.182.19	1	345.78K	0.23%	0.00%	100.00%	00:00:02	2,741	0.07%
s14.ucoz.net	11	310.29K	0.20%	0.00%	100.00%	00:00:04	4,708	0.13%
newtrax.ru	10	308.91K	0.20%	0.00%	100.00%	00:00:10	10,148	0.27%
ip.kommynist.ru	73	303.95K	0.20%	0.00%	100.00%	00:00:27	27,345	0.73%
monument.ucoz.ru	7	298.01K	0.19%	0.00%	100.00%	00:00:08	8,610	0.23%
www.sherlock-holmes.co.uk	19	280.11K	0.18%	0.00%	100.00%	00:00:10	10,278	0.27%
l-stat.livejournal.com	14	256.83K	0.17%	0.00%	100.00%	00:00:04	4,547	0.12%
gadgets.stemo.ru	28	248.72K	0.16%	0.00%	100.00%	00:00:07	7,577	0.20%
yabs.yandex.ru	48	243.93K	0.16%	23.28%	76.72%	00:00:06	6,205	0.17%
static.cache.l.google.com	22	216.37K	0.14%	0.00%	100.00%	00:00:07	7,010	0.19%
news.samaratoday.ru	7	210.37K	0.14%	0.00%	100.00%	00:00:04	4,662	0.12%
www.cprf.info	24	202.74K	0.13%	21.88%	78.12%	00:00:12	12,591	0.34%
ngbn.net	14	197.93K	0.13%	0.00%	100.00%	00:00:06	6,933	0.18%
www.anekdot.ru	31	189.50K	0.12%	0.00%	100.00%	00:00:10	10,574	0.28%
slovari.yandex.ru	10	171.85K	0.11%	0.00%	100.00%	00:00:04	4,936	0.13%
www.google.com	55	158.19K	0.10%	0.00%	100.00%	00:00:23	23,372	0.62%
src.ucoz.ru	35	156.08K	0.10%	0.00%	100.00%	00:00:09	9,175	0.24%
87.242.91.21	4	155.22K	0.10%	0.00%	100.00%	00:00:02	2,498	0.07%
www.3milliona.net	16	144.08K	0.09%	0.00%	100.00%	00:00:06	6,674	0.18%
flv.video.yandex.ru	17	136.76K	0.09%	0.00%	100.00%	00:00:02	2,727	0.07%
days.pravoslavie.ru	13	129.06K	0.08%	0.00%	100.00%	00:00:08	8,487	0.23%
gorodok.samaratoday.ru	9	125.03K	0.08%	3.71%	96.29%	00:00:07	7,637	0.20%
autocontext.begun.ru	6	123.81K	0.08%	84.75%	15.25%	00:00:00	924	0.02%
top9.mail.ru	91	118.52K	0.08%	0.00%	100.00%	00:00:08	8,069	0.21%
kommynist.ru	26	118.19K	0.08%	0.46%	99.54%	00:00:35	35,196	0.94%
img.yandex.net	44	117.74K	0.08%	21.85%	78.15%	00:00:05	5,052	0.13%
api-maps.yandex.ru	4	106.54K	0.07%	66.28%	33.72%	00:00:00	424	0.01%
nbimg.dt00.net	23	105.43K	0.07%	0.00%	100.00%	00:00:05	5,683	0.15%
video-tub.yandex.ru	22	105.06K	0.07%	0.00%	100.00%	00:00:04	4,486	0.12%
nova.rambler.ru	22	101.81K	0.07%	0.00%	100.00%	00:00:04	4,894	0.13%
counter.rambler.ru	87	97.64K	0.06%	0.00%	100.00%	00:00:11	11,428	0.30%
www.google.ru	25	96.59K	0.06%	0.00%	100.00%	00:00:09	9,914	0.26%
counter.yadro.ru	126	90.19K	0.06%	0.00%	100.00%	00:00:13	13,584	0.36%
yandex.ru	19	76.26K	0.05%	0.92%	99.08%	00:00:14	14,356	0.38%
www.lexico.ru	19	72.12K	0.05%	0.00%	100.00%	00:00:03	3,899	0.10%
87.242.91.22	6	66.72K	0.04%	0.00%	100.00%	00:00:01	1,597	0.04%
suggest.yandex.ru	112	66.12K	0.04%	15.88%	84.12%	00:00:24	24,471	0.65%
blogs.yandex.ru	27	65.74K	0.04%	0.00%	100.00%	00:00:03	3,377	0.09%
page2rss.ru	8	63.71K	0.04%	2.94%	97.06%	00:00:08	8,298	0.22%

This view shows internal IP addresses



Squid Analysis Report Generator

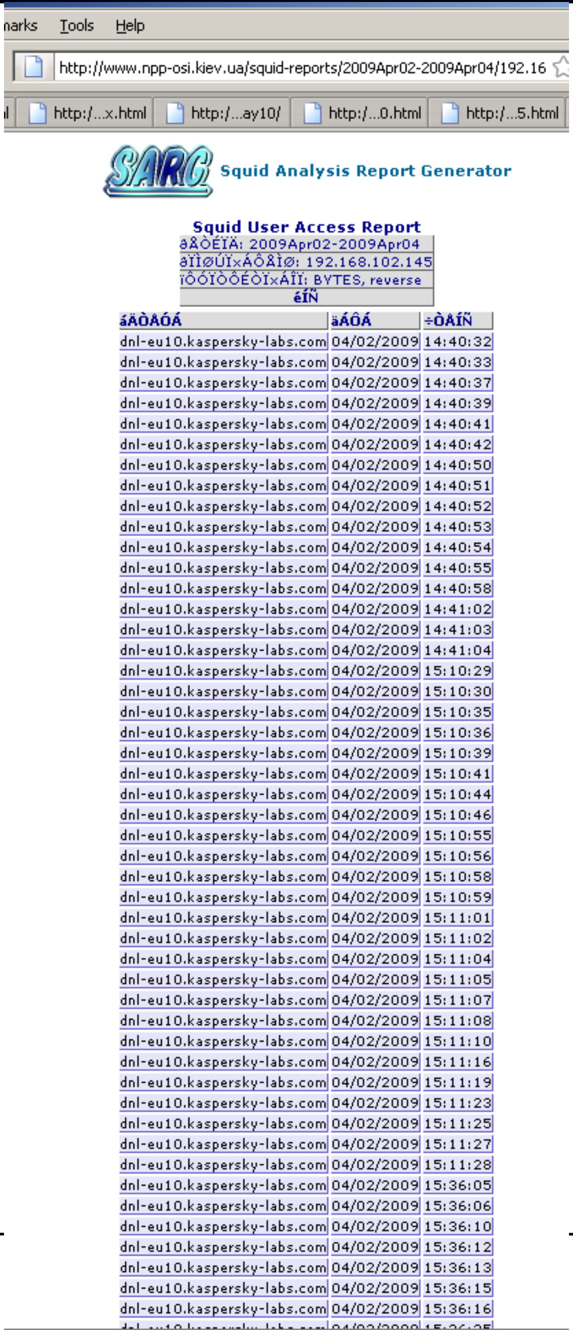
Squid User Access Report
Period: 2007May10-2007May10
Sort: BYTES, reverse
Topuser Report

Topsites Report
Sites & Users Report
Downloads Report
Denied Report

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	10.20.2.5	34.14K	1.77G	94.69%	0.00%	98.41%	00:00:00	0	0.00%
2	10.20.2.210	3.63K	47.00M	2.51%	0.00%	99.96%	00:00:00	0	0.00%
3	10.20.2.205	1.71K	19.56M	1.04%	0.00%	98.95%	00:00:00	0	0.00%
4	10.20.2.235	1.54K	8.27M	0.44%	0.00%	99.18%	00:00:00	0	0.00%
5	10.20.2.197	1.05K	7.25M	0.39%	0.00%	98.25%	00:00:00	0	0.00%
6	10.130.102.43	847	6.00M	0.32%	0.00%	97.41%	00:00:00	0	0.00%
7	10.85.72.201	800	4.84M	0.26%	0.00%	92.56%	00:00:00	0	0.00%
8	10.20.2.200	404	3.45M	0.18%	0.00%	77.44%	00:00:00	0	0.00%
9	10.20.2.80	315	2.33M	0.12%	0.00%	93.77%	00:00:00	0	0.00%
10	10.20.2.16	45	318.31K	0.02%	0.00%	79.45%	00:00:00	0	0.00%
11	10.64.130.23	96	133.24K	0.01%	0.00%	0.00%	00:00:00	0	0.00%
12	10.100.101.101	165	101.14K	0.01%	0.00%	94.48%	00:00:00	0	0.00%
13	10.20.2.2	11	66.75K	0.00%	0.00%	0.00%	00:00:00	0	0.00%
	TOTAL	44.77K	1.87G		0.00%	98.38%	00:00:00	0	
	AVERAGE	3.44K	144.00M				00:00:00	0	

Generated by sarg-2.1 Nov-29-2005 on May/10/2007 21:46

Shows what Antivirus program the target is running and how often they update



http://www.npp-osi.kiev.ua/squid-reports/2009Apr02-2009Apr04/192.16

Squid Analysis Report Generator

Squid User Access Report

ðÅÒÉÏÄ: 2009Apr02-2009Apr04

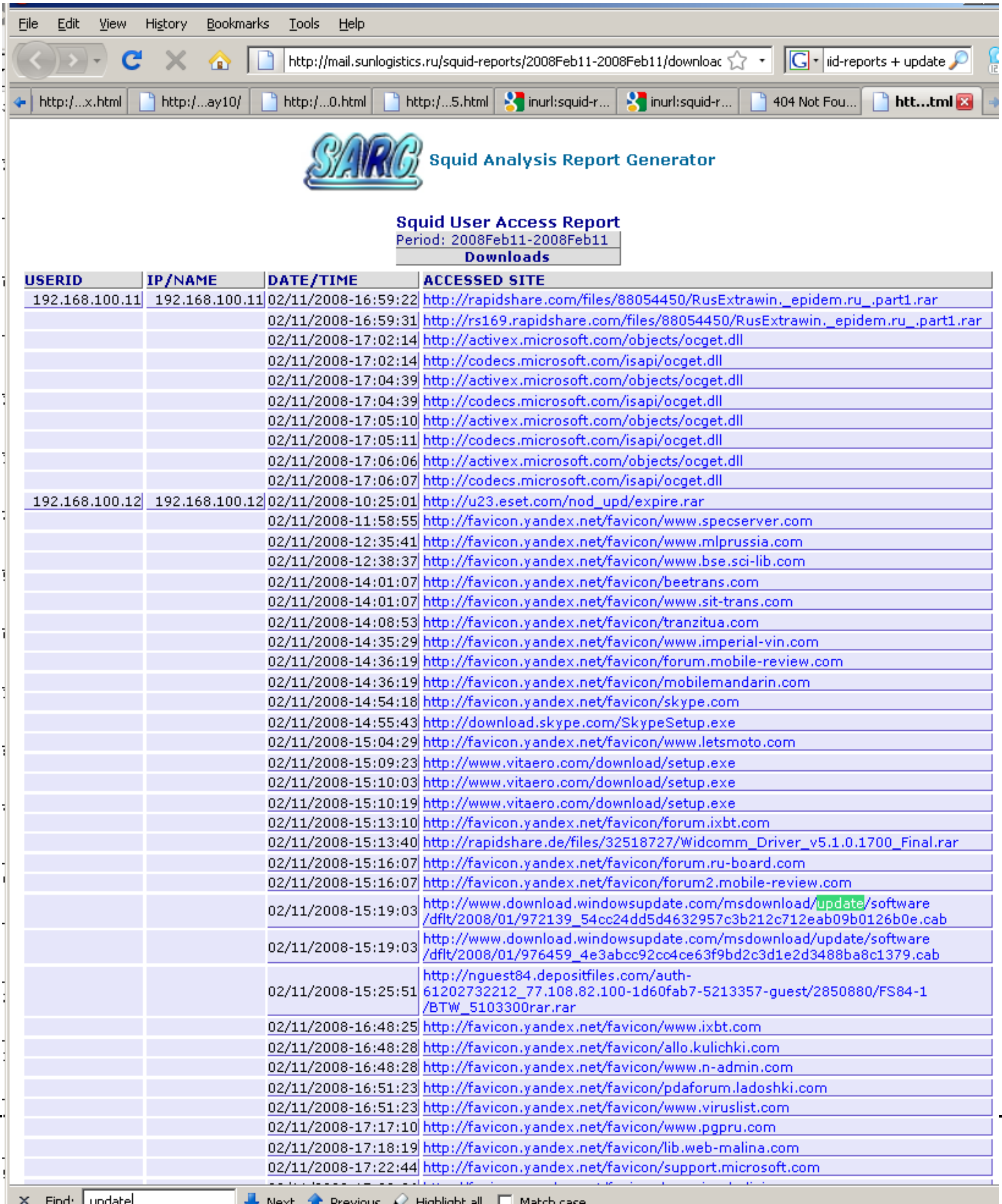
ðÏÌØÚÏ×ÁÔÅÌØ: 192.168.102.145

ïÔÓÏÒÔÉÒÏ×ÁÎ: BYTES, reverse

éÍÑ

áÄÒÅÓÁ	äÁÔÁ	÷ÒÅÍÑ
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:32
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:33
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:37
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:39
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:41
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:42
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:50
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:51
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:52
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:53
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:54
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:55
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:58
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:02
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:03
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:04
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:29
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:30
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:35
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:36
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:39
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:41
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:44
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:46
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:55
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:56
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:58
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:59
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:01
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:02
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:04
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:05
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:07
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:08
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:10
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:16
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:19
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:23
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:25
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:27
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:28
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:05
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:06
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:10
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:12
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:13
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:15
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:16

Shows that target is running Microsoft windows and gives hints as to what updates are being installed as well as frequency of update



Squid Analysis Report Generator

Squid User Access Report
Period: 2008Feb11-2008Feb11
Downloads

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
192.168.100.11	192.168.100.11	02/11/2008-16:59:22	http://rapidshare.com/files/88054450/RusExtrawin._epidem.ru_.part1.rar
		02/11/2008-16:59:31	http://rs169.rapidshare.com/files/88054450/RusExtrawin._epidem.ru_.part1.rar
		02/11/2008-17:02:14	http://activex.microsoft.com/objects/ocget.dll
		02/11/2008-17:02:14	http://codecs.microsoft.com/isapi/ocget.dll
		02/11/2008-17:04:39	http://activex.microsoft.com/objects/ocget.dll
		02/11/2008-17:04:39	http://codecs.microsoft.com/isapi/ocget.dll
		02/11/2008-17:05:10	http://activex.microsoft.com/objects/ocget.dll
		02/11/2008-17:05:11	http://codecs.microsoft.com/isapi/ocget.dll
		02/11/2008-17:06:06	http://activex.microsoft.com/objects/ocget.dll
		02/11/2008-17:06:07	http://codecs.microsoft.com/isapi/ocget.dll
192.168.100.12	192.168.100.12	02/11/2008-10:25:01	http://u23.eset.com/nod_upd/expire.rar
		02/11/2008-11:58:55	http://favicon.yandex.net/favicon/www.specserver.com
		02/11/2008-12:35:41	http://favicon.yandex.net/favicon/www.mlprussia.com
		02/11/2008-12:38:37	http://favicon.yandex.net/favicon/www.bse.sci-lib.com
		02/11/2008-14:01:07	http://favicon.yandex.net/favicon/beetrans.com
		02/11/2008-14:01:07	http://favicon.yandex.net/favicon/www.sit-trans.com
		02/11/2008-14:08:53	http://favicon.yandex.net/favicon/tranzitua.com
		02/11/2008-14:35:29	http://favicon.yandex.net/favicon/www.imperial-vin.com
		02/11/2008-14:36:19	http://favicon.yandex.net/favicon/forum.mobile-review.com
		02/11/2008-14:36:19	http://favicon.yandex.net/favicon/mobilemandarin.com
		02/11/2008-14:54:18	http://favicon.yandex.net/favicon/skype.com
		02/11/2008-14:55:43	http://download.skype.com/SkypeSetup.exe
		02/11/2008-15:04:29	http://favicon.yandex.net/favicon/www.letsmoto.com
		02/11/2008-15:09:23	http://www.vitaero.com/download/setup.exe
		02/11/2008-15:10:03	http://www.vitaero.com/download/setup.exe
		02/11/2008-15:10:19	http://www.vitaero.com/download/setup.exe
		02/11/2008-15:13:10	http://favicon.yandex.net/favicon/forum.ixbt.com
		02/11/2008-15:13:40	http://rapidshare.de/files/32518727/Widcomm_Driver_v5.1.0.1700_Final.rar
		02/11/2008-15:16:07	http://favicon.yandex.net/favicon/forum.ru-board.com
		02/11/2008-15:16:07	http://favicon.yandex.net/favicon/forum2.mobile-review.com
		02/11/2008-15:19:03	http://www.download.windowsupdate.com/msdownload/update/software /dflt/2008/01/972139_54cc24dd5d4632957c3b212c712eab09b0126b0e.cab
		02/11/2008-15:19:03	http://www.download.windowsupdate.com/msdownload/update/software /dflt/2008/01/976459_4e3abcc92cc4ce63f9bd2c3d1e2d3488ba8c1379.cab
		02/11/2008-15:25:51	http://nguest84.depositfiles.com/auth-61202732212_77.108.82.100-1d60fab7-5213357-guest/2850880/FS84-1 /BTW_5103300rar.rar
		02/11/2008-16:48:25	http://favicon.yandex.net/favicon/www.ixbt.com
		02/11/2008-16:48:28	http://favicon.yandex.net/favicon/allo.kulichki.com
		02/11/2008-16:48:28	http://favicon.yandex.net/favicon/www.n-admin.com
		02/11/2008-16:51:23	http://favicon.yandex.net/favicon/pdaforum.ladoshki.com
		02/11/2008-16:51:23	http://favicon.yandex.net/favicon/www.viruslist.com
		02/11/2008-17:17:10	http://favicon.yandex.net/favicon/www.pgpru.com
		02/11/2008-17:18:19	http://favicon.yandex.net/favicon/lib.web-malina.com
		02/11/2008-17:22:44	http://favicon.yandex.net/favicon/support.microsoft.com

OWN3D
OWN3D
debian
OWN3D
OWN3D

Profiling

- How White Hats get **assigned** Targets:
  - "Only touch xyz hosts, don't touch abc, those are production“
  - "Hosts 123 we already know are vulnerable, don't worry about those"

- How Black Hats **Choose** Targets:
  - Source code devs
  - Pen testers
  - Researchers
  - Maintain Control
  - May not yield access immediately

Analysis of Black Hat Techniques in the Wild

- **Environment Modeling & Testing**
  – White hats test attacks against clients
  – We have seen whole environments mirrored
  – Base mock up on info gathering
    - Match OS, hardware, patch levels, applications
    - Virtualization up to real hardware
- **Exploit Development**
  – Black Hats write them
  – White Hats use them

Analysis of Black Hat Techniques in the Wild

- **Flexible Environment Testing**
  - Can do vulnerability assessment at leisure
    - Code auditing
      - Double win: 0day + 0wnage
    - Fuzzing
    - Reverse Engineering / Binary Analysis
  - Exploit testing without alerting target
  - One case was 18 months of staging
    - Less than 1 minute of exploitation
    - 5 minutes of data stealing

Analysis of Black Hat Techniques in the Wild

- **Examples**
  - Attack on Apache.org
  - Attack on Debian.org
  - Attack on Wordpress.com
  - Attack on Comcast.net
  - Attack on Linux Distro
  - Attack on Bank

Analysis of Black Hat Techniques in the Wild

- **Apache.org**
  - Attackers used no exploits. Instead they relied on configuration errors
  - Used a combination of small bugs leveraged against the system to gain
  - Administrative access to the main source repository
  - Patiently waited for root to login.
  - Defaced

Analysis of Black Hat Techniques in the Wild

- **Debian.org**
  - Attackers used no exploits.
  - SSH Authkey misuse on a system in Japan and a system in the Netherlands
  - Allowed access to the administrative account on debian.org
  - SSHD backdoored and core debian OS source backdoored
  - Was unknown for 6 months

Analysis of Black Hat Techniques in the Wild

- **Wordpress.com**
  - Attackers used zero day vulnerability
  - Backdoored Live web application
  - Accessed chief source code repository
  - Backdoored source code
  - Was quickly noticed and fixed

Analysis of Black Hat Techniques in the Wild

- **Comcast.net**
  - Attackers used no exploits
  - Attackers Social Engineered Network Solutions into granting them access to Comcast's account
  - Attackers redirected comcast.net domain name to attacker controlled servers
  - Defaced

Analysis of Black Hat Techniques in the Wild

- **Major Linux Distro**
  - Heard of attacker getting in over months
  - Subtlety backdoored distro
    - Introduced bug
  - Matched md5s
  - Able to own any system for 6 months
  - Distro NOT the ultimate target

Analysis of Black Hat Techniques in the Wild

- **Hackme Bank**
  - Found devel host on separate network
  - Attackers used custom vuln in co-located website
  - Read many files via directory traversal
    - Solaris treats directories like files
      - So you can do cat dir/ and get an ls
  - Discovered copy of every transaction goes over email
  - Copied mail spool via targets own website
  - $$$$

Analysis of Black Hat Techniques in the Wild

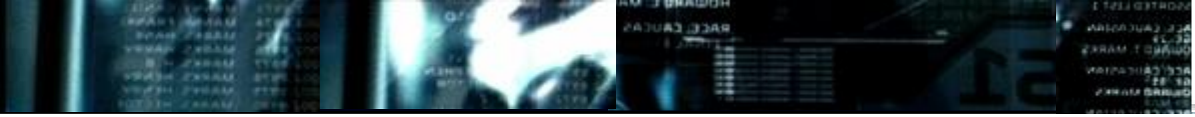
- **Air Gap**
  - Difficult to hack network w/ smart admins
  - Attackers did recon, read target procedure docs
    - Two networks
      - One online, heavily monitored
      - One offline exact copy cold backup
      - One tape drive machine for copying back and forth
  - Compromised tape system (nothing else vuln)
    - Found 0day in unix TAR
    - Generated a malicious TAR file header
    - Payload wrote malicious binaries into archive

Analysis of Black Hat Techniques in the Wild

- **Air Gap**
  - Exploit had to reload TAR and start untarring from an offset pointing to valid archive
    - Execution continuation
  - Admins eventually moved trojaned backups to “cold” side
  - Attacker made loud (but ineffective) attacks on “hot” side
  - Admins assumed compromise and restored “hot” side from cold backups
    - Thus trojaning their own systems and giving attacker access

Analysis of Black Hat Techniques in the Wild

- **Banking backbone**
  - Attacker stumbled upon system while doing x25 scans
  - Old ftp / ftp uname & password trick worked for a shell
  - Attacker poked around system and noticed financial transactions
    - LARGE amounts of money
    - Grabbed docs and logged out
  - Turn out to be major banking transaction system
    - All transactions encrypted, but banks would ftp transaction logs to server and store them clear text for balance reconciling
  - By coincidence attacker met system owner in real life
  - Caused no damage, but spent a year hiding



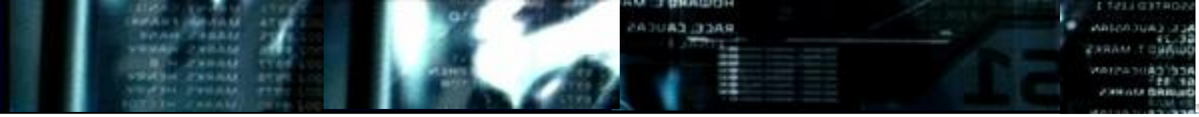
Analysis of Black Hat Techniques in the Wild

- **University**
  - Attacker compromised system at major university
  - Forensics discovered the compromise
  - Attacker used a kernel rootkit years before common
    - Investigators assumed nation state sponsored attack
    - It wasn’t
    - Rootkit removed
  - Attacker spent 6 – 8 months designing a bios rootkit
  - Re-compromised system and went undetected with new technique
  - Illustrates persistence of some attackers

Black Hat Techniques De-Mystified

Black Hat Techniques De-Mystified

- **Few exploits used in attacks**
  - Often only 1 exploit needed
  - Rest is captured passwords
  - Trust hijacking
  - Using compromised user's access
    - Datacenter / SSH example
    - authorized_keys infection



Black Hat Techniques De-Mystified

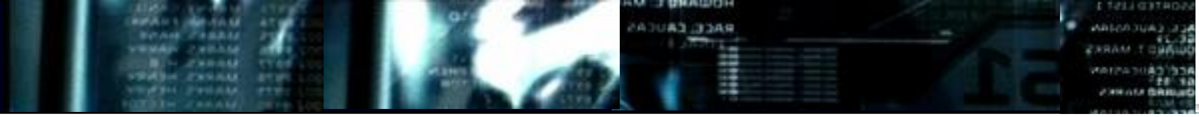
- **Few exploits used in attacks**
  - Looking like a normal user is hard to detect
    - No shellcode / payloads for IDS to see
    - Traffic looks like normal user activity
  - 0day is priceless
    - Often used when 1day
  - Greater knowledge of system internals is key
  - Attackers know your playbook
    - Blackhats don't do what pen testers do
    - (Unless they want to look like you)

Black Hat Techniques De-Mystified

- **Problems attackers run into**
  - Secure Data Exfiltration
  - Dangerous Data
    - Mail spools full of viruses
    - Smart targets, documents with attribution call homes
    - Trojaned TAR files
      - Built to overwrite home directories
  - Burn data to CD
  - Read offline on throw away box
    - Avoids above problems

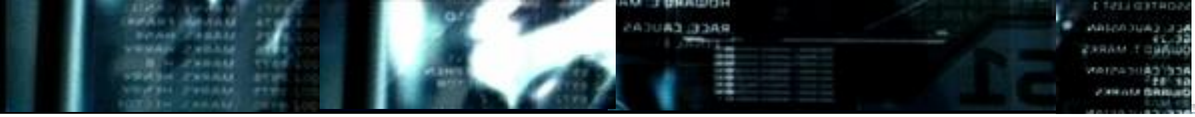
Black Hat Techniques De-Mystified

- **Problems attackers run into**
  - Retrieving GB's over Tor
  - Download managers not just for warez
  - Scripted Tor wget's
  - POST's instead of GET's
  - Obfuscates logs
  - How to get reverse shells back without attribution?
  - Leaking info during attack (emails / chats)



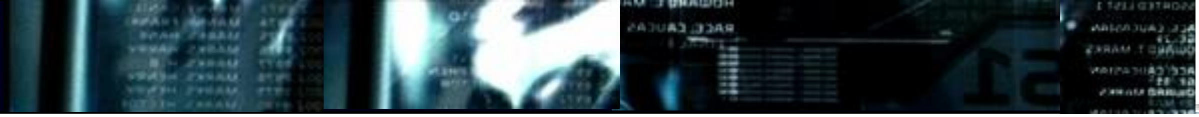
Black Hat Techniques De-Mystified

- **Maintaining Control**
  - Data Interception is priority number one.
    - Let the victims do the hacking for you
  - Why use rootkits
    - Detectable
    - Kernel behavior almost always indicates 0wnage
  - Better to ensure re-exploitation at will
  - Hide in plain site / look like normal activity



Black Hat Techniques De-Mystified

- **Maintaining Control**
  - Introduce subtle bugs instead of backdoor binaries
  - Modify source to be vulnerable
    - Harder to detect than blatant backdoor
  - Downgrade applications to vuln versions
  - Re-enable disabled accounts
  - Keep admins & incident response second guessing
    - Flood box with worms & malware if you don't get in
    - Hide in the noise



Black Hat Techniques De-Mystified

- **Maintaining Control**
  - Example:
  - Machine has VNC installed
  - Replace installed VNC with vulnerable version
    - Authentication bypass
  - Copy registry password so target doesn’t realize software has been updated
  - Persistence with no malware or rootkits to get detected

- **Maintaining Control**
  - Add vulnerable code
  - Example: web apps
    - Take out user input validation
    - Inject your vulnerable code
      - Focus on vague intent
      - Never be obviously and solely malicious
    - Look for apps with previous vulnerabilities
    - Re-introduce patched bugs

- **Maintaining Control**
  - More web app examples
  - Add hidden field to HTML form
    - Users detect no change, app performs normally

```
<input type=“hidden” name=“Lang”>
```

  - Edit web app and tie vuln perl code to form field input

```
If defined $hidden_field {
        open($filename,”>$hidden_field”);
}
```

  - Craft a POST including the hidden field

- **Maintaining Control**
  - www.target.com/cgi-bin/app.cgi?lang=|cmd|
  - Code will execute your commands
  - Who needs to bind a shell to a port?
  - Unlikely to ever be detected
    - Especially good in big apps
    - Code review can’t ever be sure of maliciousness
    - But some sites replace code every X time-period
  - No rootkits to install
  - Unusual to tripwire all web code

Black Hat Techniques De-Mystified

- **Other Attackers**
  - – Find them on the target
  - – Full intrusion analysis
  - – Understand what they have done and what they are after
    - Maybe a box you didn't think was important actually is
  - – Model your behavior after them
  - – Make your activity look like they did it
  - – Find and patch the hole they used to get in
    - Kick them out

Black Hat Techniques De-Mystified

- **Other Attackers**
  - Example
    - One case found another attacker on same box
    - Had modified login script
    - Exclude logins from attack host from logging
    - Added self as well to same script

Black Hat Techniques De-Mystified

- **Protecting Bugs**
  - Example
    - Attacker had 0day for commonly used service
    - Rumors circulated
    - Attacker had a colleague leak a different, less reliable but related bug
    - Removed focus from attacker and real bug
      - CMD Exec survived another 4 years

Black Hat Techniques De-Mystified

- **Anonymity**
  - Hijack wifi
  - Look for default configured u/p WAPs
  - Modify DMZ to get reverse shells back
  - Find web shells on boxes other people hacked
    - Use them as launch pads
    - You didn’t even have to hack them yourself

Black Hat Techniques De-Mystified

- **Anonymity**
  - Tor
    - Hide in the Tor noise
    - Porn, warez & hacking
    - Do all recon possible in Tor or similar
    - Change IP's (Identities) often
    - Use 3rd party web based port scanners
    - Hit target and web tools only from Tor

Black Hat Techniques De-Mystified

- **Anonymity**
  - Tor C&C
    - See Metaphish Talk
    - 100% True SSL encrypted
    - Cross platform
      - Mono
      - Linux & Windows with same binary
    - Communicates using Tor hidden services
    - Even if target:
      - Reverses backdoor
      - Has 100% packet capture
      - They cannot trace it back to source

Black Hat Techniques De-Mystified

- **Anonymity**
  - – Covert communications
  - – Attackers use strange covert communications
  - – Example
    - Edonkey p2p with crypto enabled appears to simply be SSL traffic
    - Some attackers known to use this for file transfer and communications
    - In one case TCP over edonkey
  - – Have seen attackers using twitter, gmail and msn messenger for command and control of compromised systems

Never Caught

Never Caught

- **Anti-forensics & Law Enforcement**
  - Cell phone alibi
    - Place phone in desired location away from attack
    - Have call made to phone
    - Have phone answered
      - Accomplices bring complications
    - Auto answer programs for smart phones
    - When phone records are pulled:
    - Location + call record "prove" your location
  - Buy a movie ticket & leave movie early
  - Whole field of study: Alibiware

Never Caught

- **Anti-forensics & Law Enforcement**
  - Reset every timestamp on system to same date
    - Timestomp
  - Encase exploits
  - Memory only & staged C&C
    - Just enough code to receive next chunk from network
    - True SSL
    - Need full packet capture + break SSL to get C&C analysis
    - No real malware on disk to RE

Never Caught

- **Data protection & destruction**
  - Attackers have to protect their data from other attackers and law enforcement
    - Some attackers encrypt all data with complex key
    - One group of attackers built a drive “chipper”
    - 1 ½ horse power motor from a metal router
    - Metal router blades
    - Result a giant bin full of no bigger than ½ inch square drive parts
    - Good luck getting forensic data

What does all this mean?

What does all this mean?

- Attackers are determined
  - They will not stop
- Attackers are extremely patient
- Only have to succeed once
- Understand how an attacker thinks
- Know your Enemy
- Test everything
  - Small bugs yield Big bugs

- Black Hats are not all powerful
  - They just know more tricks

- Many pen testers are providing **unrealistic** tests

- **Full scope best value**

What does all this mean?

- **What can you do?**
  - Proper Training
  - Investigate Reports
  - Identify Targets
  - Predict Attackers
  - Proactive Defense is best
  - Defense is not System Administration
  - Properly Mitigate Risk
  - Learn from other peoples mistakes
  - Open Discussion