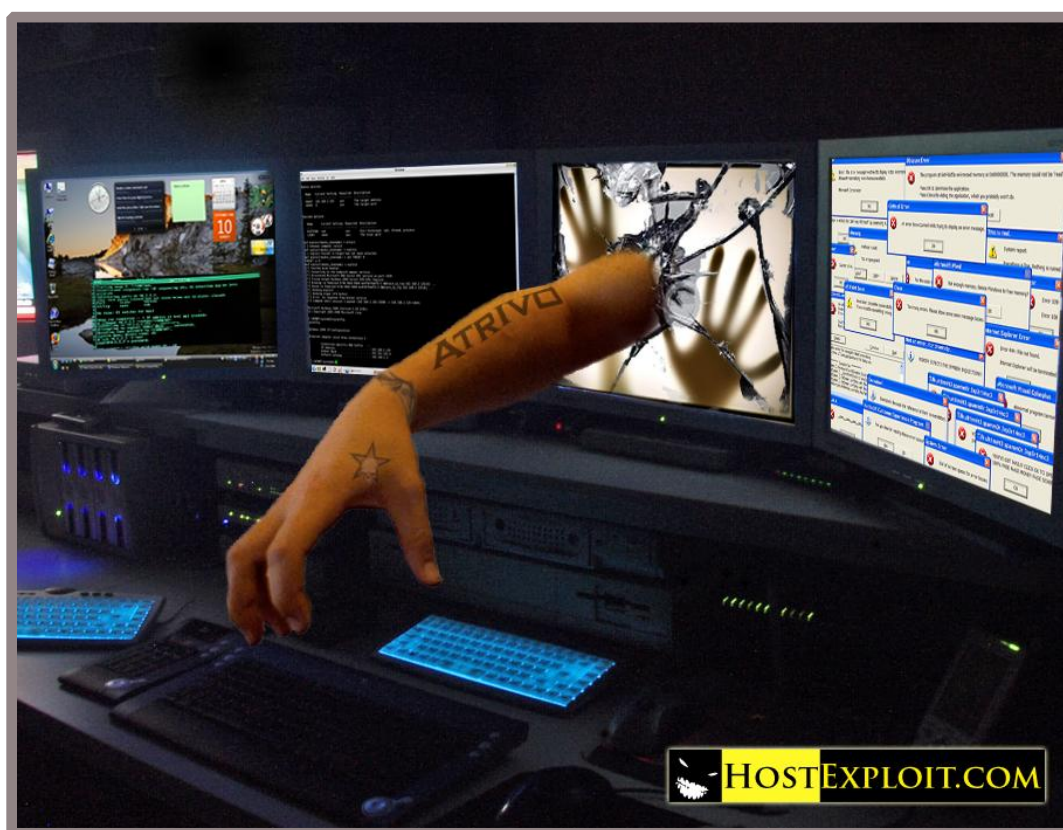


Atrivo – Cyber Crime USA

White Paper - Atrivo and their Associates



Jart Armin,
September 2008 – Vers: 1.1

In Association with: James McQuaid, and Matt Jonkman

Technical Review: Bob Bruen, David Bizeul

With the help and assistance of many 'concerned netizens' within the Internet
and Open Source Security community.

ATRIVO – CYBER CRIME USA

White Paper - Atrivo and their Associates

Abstract

This study was initiated to track and document scientifically the ongoing cyber criminal activity from within the IP space and servers controlled by the California-based Atrivo, and other associated entities. Atrivo is a significant Service Provider and peering point on the Internet, and controls a large number of IP addresses used to serve content end users all over the world. The philosophy behind this study is the fear that either we as an Internet community take action to 'stop' the cyber criminals or the average user will increasingly clamor for governmental controls or seek a closed Internet to protect them.

This is an Open Source Security study set out to quantify and continuously track cyber crime using numerous methods of measurement. It focuses specifically on the notorious Atrivo, which has been seen by many over several years as a main conduit for financial scams, identity theft, spam and malware. This study although fully self contained is the first of a series of reports, on a monthly basis there will be a follow up to report on the community response, the efforts of the cyber criminals to evade exposure, listings to assist in blocking the risks to Internet users, and hopefully efforts to stop them.

In addition to original quantitative research the study draws upon the findings of other research efforts, including StopBadware, Emerging Threats, Knujon, Sunbelt, CastleCops, Spamhaus, and many others. What emerges is a picture of a front for cyber criminals, who have specifically targeted consumers in the United States and elsewhere. The study provides hard data regarding specific current activity within Atrivo, explains how consumers are targeted, describes Atrivo's virtual network structure, organizational modeling, and cites Atrivo's collusive failure to respond to abuse complaints from 2004 to the present.

Version 1.1 – Updated; notes Pages 4 /5 & Pages 11 – Updated; PrivacyProtect.org Pages 8 /9 – Updated sample of specific report references

Introduction

In Jonathan Zittrain's "The Future of the Internet and How to Stop It" he states:

"Today, the same qualities that led to the success of the Internet and general-purpose PCs are causing them to falter. As ubiquitous as Internet technologies are today, the pieces are in place for a wholesale shift away from the original chaotic design that has given rise to the modern information revolution. This counterrevolution would push mainstream users away from the generative Internet that fosters innovation and disruption, to an applianceized network that incorporates some of the most powerful features of today's Internet while greatly limiting its innovative capacity—and, for better or worse, heightening its regulability. A seductive and more powerful generation of proprietary networks and information appliances is waiting for round two. If the problems associated with the Internet and PC are not addressed, a set of blunt solutions will likely be applied to solve problems at the expense of much of what we love about today's information ecosystem."

The inexorable rise of ID theft, malware, viruses, spam, or let us generally call it 'Badware' provides a potential threat to the 'generative' Internet. This study is dedicated to the view we as the Internet community i.e. the 'concerned netizens' can resolve our own problems.

So why Atrivo et. al. ? Perhaps the most appropriate is to quote from one of Spamhaus' the well known anti-spam organization's many listings;

"Atrivo / Intercage - Spammer/cybercrime hosting front - Inhoster.com?... aka Esthost?... aka Estdomains... aka Cernal?... aka ? Via Emil at Atrivo/Intercage...Too much spam and crime - routing must cease".

Atrivo is a major hub of cyber crime based within the USA, and has been known as such within the Internet community for many years. Within this study we provide detailed evidence not only for public and community awareness but also to provide evidence for action.

It should be stressed such activities could not occur if commercial third parties or other organizations did not collaborate. Such collaboration maybe and often is the equivalent of turning a blind eye to the bad activity but accepting the cash as perhaps several commercial hosting or Internet servers do, or acceptance of sponsorship and entertainment. However within a conventional criminal comparison the supplier of the unregistered handgun used in a crime, is also responsible for that crime?

PC User Exploitation Video:

[HostExploit video page](#)

[You Tube](#)

Section 1: Atrivo – Mapping the Problem

So the first logical step is to identify the various elements of Atrivo. Again, it is important to remember Atrivo does not exist in isolation; it must gain wider access to the internet, dodge the spam blacklists, rent added server (rack) space, and get paid for the privacy and efficient hosting it provides the hackers and cyber criminals. Below in figure 1.1 we show the core components of Atrivo with examples of how and who they link with.

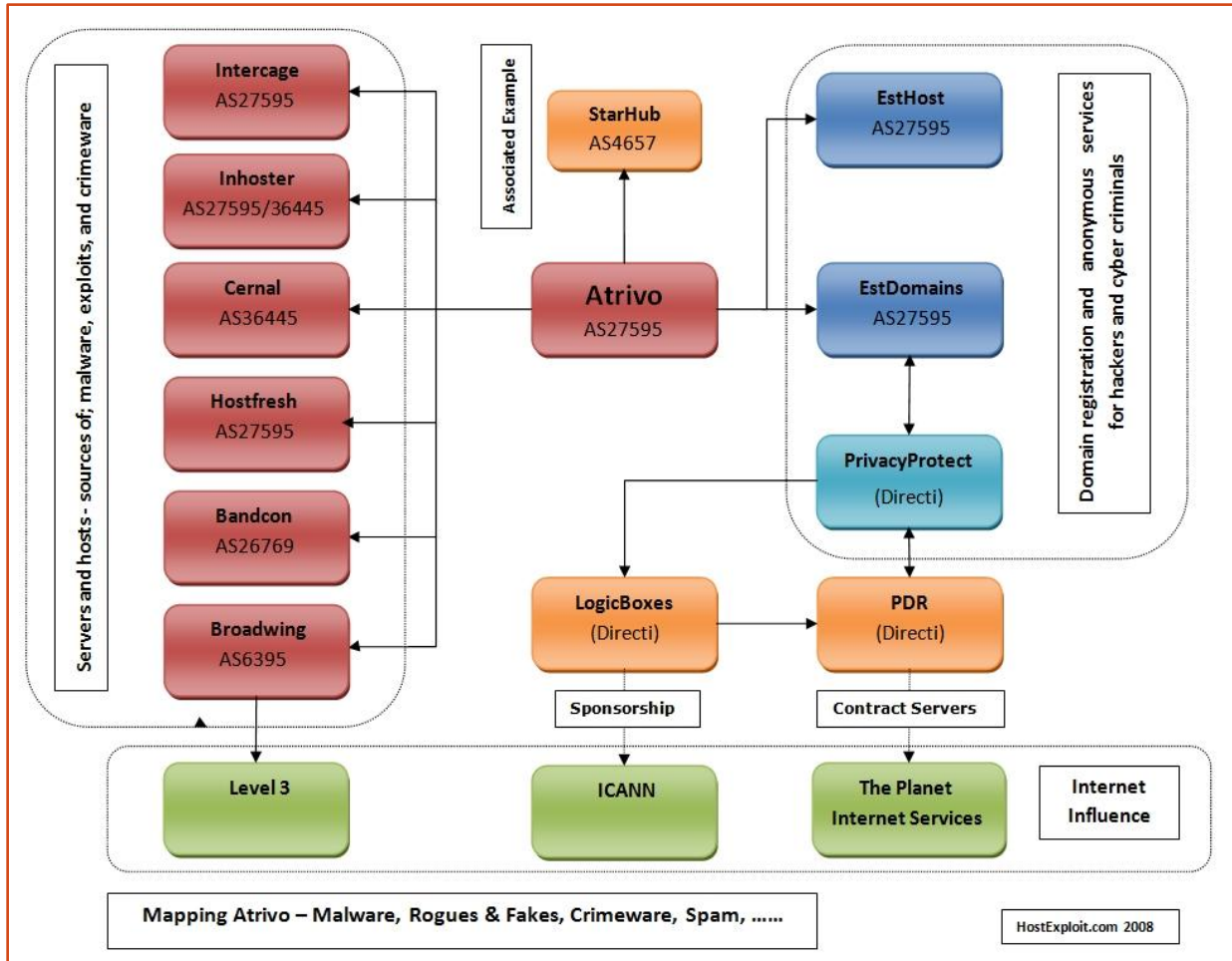


Figure 1.1 – Mapping Atrivo

Atrivo's reach in the cyber crime community and the Internet as a whole runs deep. From their partners in crime, to the domain registration and hosting services it has to be remembered this is deliberately misleading to avoid detection. In conjunction with figure 1, below we provide the overlapping linkage and clarification:

Figure 1.1 shows a color coded form of key: The specifics of the individual elements of the figure are shown below.

Atrivo Services (left hand side fig1.1)



Intercage – AS 27595 (as Atrivo) - Alexa rank of 4,773 – 12-custblock.intercage.com - 97% of traffic.

	Record	Name	IP Address	AS
intercage.com	a		216.255.187.125	AS27595 ATRIVO AS Atrivo
	ns	ns3.intercage.com	69.50.182.162	
		ns4.intercage.com	69.50.182.163	
		ns1.intercage.com	216.255.187.122	
		ns2.intercage.com	216.255.187.123	
mx	xcaliber.intercage.com	216.255.187.122		

Also see Spamhaus lasso [SBL53802](#)

Also linked to WvFibre, Inhoster,

For example home of fake and rogue anti-spyware / anti-virus MalwareAlarm, Spyshredder, (See section



Inhoster – (AKA UkrTeleGroup) a base for Ukraine server operation

85.255.112.0-85.255.127.255 UkrTeleGroup UkrTeleGroup Ltd.	
85.255.112.0/20 Cernel Network Ltd	
AS36445 CERNEL Network Ltd	
85.255.112.0/24 Pilosoft, Inc	
AS36445 CERNEL Network Ltd	
85.255.112.0-85.255.127.255 UKkrTeleGroup UkrTeleGroup Ltd.	
Http:Apache/1.3.37 (Unix)	mail.inhoster.com
PHP/4.4.4	ns2.ukrtelegroup.com.ua

Also see Spamhaus lasso [SBL36453](#)

Rev 1.1 Note: It should be noted the routing of 85.255.112.0/24. It is reported to the authors Pilosoft severed the relationship apparently via EstHost during July 2008. The table above reflects analysis over the several months of observation before this report was published.

Atrivo
Services

Cernal – AS 36445 – routed via AS 27595 Atrivo

AS36445 CERNEL Network Ltd			
in bgp	Route record	Prefix	Description
AS27595 AS26769	AS27595 AS36445	64.28.176.0/20	BNDAS-INC-IP-SFO1-001 Atrivo Cernel Network Ltd
		85.255.112.0/20	Cernel Network Ltd.
AS36445 AS26627		85.255.112.0/24	Pilosoft, Inc.

Also see Spamhaus <http://www.spamhaus.org/sbl/sbl.lasso?query=SBL36453>

Rev 1.1 Note: It should be noted the routing of 85.255.112.0/24. It is reported to the authors Pilosoft severed the relationship apparently via EstHost during July 2008. The table above reflects analysis over the several months of observation before this report was published.

Atrivo
Services

Hostfresh – AS 27595 Atrivo, using a P.O. Box in Hong Kong for gaining and routing traffic via China

	Record	Name	IP Address	AS
hostfresh.com	a		58.65.238.99	AS27595 ATRIVO AS Atrivo
	ns	ns1.hostfresh.com	58.65.238.100	
		ns2.hostfresh.com	58.65.238.101	
	mx	hostfresh.com	58.65.238.99	

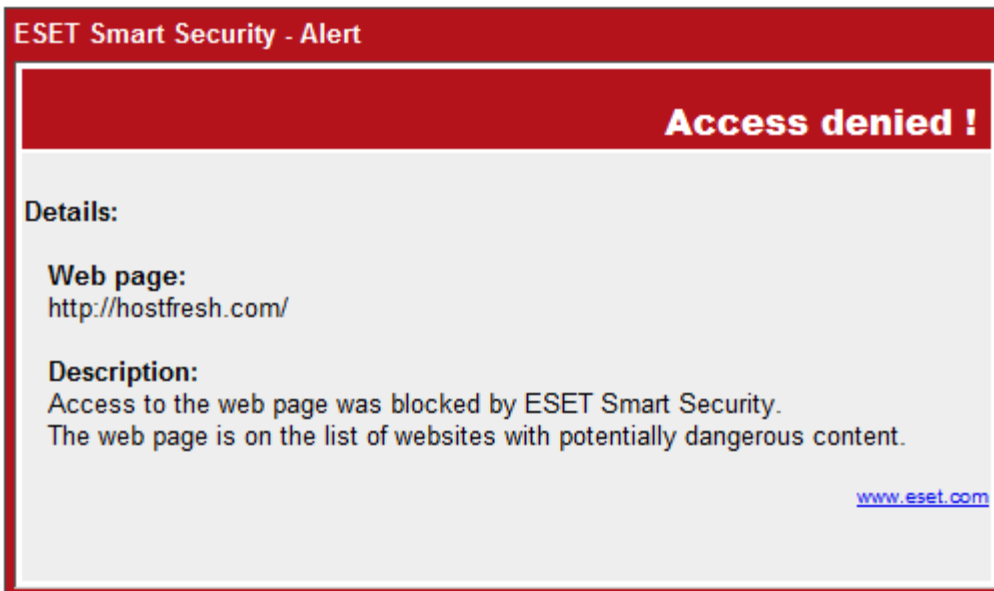


Fig 1.2 Demonstrates PC user based defense – Eset Corp. – Nod 32

Atrivo Services

Bandcon – AS 26769 - One of Atrivo’s core providers of backbone Internet provision

NET 64.28.176.0/20	
origin:	AS36445(CERNEL Network Ltd)
descr:	Cernel Network Ltd.
descr:	Atrivo
origin:	AS27595(ATRIVO AS Atrivo)
descr:	BNDAS-INC-IP-SFO1-001
origin:	AS26769(BANDCON Bandcon)

Atrivo Services

Broadwing – AS 6395 - Acquired by Level3 Communications (NASDAQ: LVLT) in Jan 2007, another of Atrivo’s core providers of backbone Internet provision.

69.22.184.0-69.22.187.255 InterCage, Inc. LITEUP-69-22-184-0-1 (NET-69-22-184-0-2)
69.22.184.0/22 Broadwing Communications, LLC 1122 Capital of Texas Highway South Austin, TX 78746 Atrivo
AS27595 ATRIVO AS Atrivo

Atrivo Associated Example (top of fig 1.1)

StarHub AS4657

StarHub – AS 4657 Singapore based providing collocation for Atrivo

	Record	Name	IP Address	AS
ns1.malware-alarm.com	a		203.117.175.116	AS4657 STARHUBINTERNET AS Starhub Internet Pte Ltd 31, Kaki Bukit Rd 3 SINGAPORE (previously known as CyberWay Pte Ltd)
*.malware-alarm.com	a	malware-alarm.com	220.196.42.220	AS9800 CHINAUNICOM BACKBONE No 133, Xi'dan North Street Beijing 100032
malware-alarm.com	a		220.196.42.220	AS9800 CHINAUNICOM BACKBONE No 133, Xi'dan North Street Beijing 100032
	ns	ns1.malware-alarm.com	203.117.175.116	AS4657 STARHUBINTERNET AS Starhub Internet Pte Ltd 31, Kaki Bukit Rd 3 SINGAPORE (previously known as CyberWay Pte Ltd)
		ns2.malware-alarm.com	124.217.252.78	AS9930 TINET MY TIMEDOTCOM BERHAD
	mx	mail.malware-alarm.com	69.50.167.172	AS27595 ATRIVO AS Atrivo

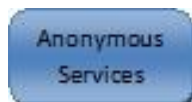
The Anonymous Services (right of fig 1.1)

A further key factor for cyber crime is anonymity, the most important of these Atrivo associations is, EstDomains (anonymous registrant), EstHost (anonymous hosting), PrivacyProtect (anonymous registrant), LogicBoxes (hosting servers). It is an interesting background

Rather than an elaborate explanation in this version of the study, we use a few simple community quotes:

- (a) **Spam:** 76.09% - 35 of 46 active domains appearing in (spam) email which are registered at ESTDOMAINS, INC. are listed by URIBL in the last 5 days. (URIBL - 08/28/08)

- (b) **Fake Codec web sites:** Most importantly all 113 domains are or were registered with Estdomains, similarly all of the active 53 domains are hosted by AS27595 by Atrivo; AKA – Interage, Inhoster, Cernal, etc. Also added should be AS 36445 a newer Autonomous Server apparently used by Cernal. (RBNexploit and Sunbelt - Oct 2007)



EstDomains

estdomains.com				
base	record	name	ip	as
estdomains.com	a		216.255.176.238	AS27595 ATRIVO
	ns	ans2.esthost.com	216.255.183.125	
		ans1.esthost.com	216.255.183.122	
		ns1.estdomains.com	69.50.176.228	
		ns2.estdomains.com	216.255.190.84	
	mx	meduza2.esthost.com	69.50.176.226	

880 EstDomains domains advertised through spam, most are of the fake pharmacy variety. (Knucion)

Anonymous Services

EstHost

esthost.com				
base	record	name	ip	as
esthost.com	a		216.255.189.90	AS27595 ATRIVO
	ns	ans2.esthost.com	216.255.183.125	
		ens1.esthost.com	69.50.176.229	
		ans3.esthost.com	64.28.187.5	AS36445 CERNEL
		ans4.esthost.com	67.210.12.66	
	mx	mail1.esthost.com	69.50.176.226	AS27595 ATRIVO

Anonymous Services

PrivacyProtect

	Record	IP	Reverse	Route	AS
privacyprotect.org	a	209.62.85.54	209-62-85-54. opticaljungle.com	209.62.64.0/18	AS36420
209-62-85-54. opticaljungle.com	ptr			ThePlanet	Everyones - Internet3

20,290 PrivacyProtect registered domains reported as advertised in spam.

For the ones that are active and have been scored:

- 49% are software piracy
- 30% fake pharmacy/enhancement/etc.
- 19.5% Are knockoff luxury goods

2,733 of these are PDR

821 of these are EstDomains

Until recently Dynamic Dolphin was the biggest user of this service with 5,143 recorded (Knujon)

```
JavaScript - http://privacyprotect.org/about-privacyprotection/?PHPSESSID=31c35476911a5efcc11728226a078b25
* Collapse All
* Expand All
http://privacyprotect.org/about-privacyprotection/?PHPSESSID=31c35476911a5efcc11728226a078b25
http://privacyprotect.org/ui/js/milonic_src.js
/*
Milonic DHTML Menu - JavaScript Website Navigation System.
Version 5.770 - Built: Thursday February 1 2007 - 11:28
Copyright 2007 (c) Milonic Solutions Limited. All Rights Reserved.
This is a commercial software product, please visit http://www.milonic.com/ for more information.
See http://www.milonic.com/license.php for Commercial License Agreement
All Copyright statements must always remain in place in all files at all times
***** PLEASE NOTE: THIS IS NOT FREE SOFTWARE, IT MUST BE LICENSED FOR ALL USE *****
License Details:
Number: 198259
URL: http://www.logicboxes.com
Type: Worldwide
Dated: Tuesday May 24 2005
```

Fig 1.3 Shows a screen capture from the PrivacyProtect web site HTML code –

Note: [the license to LogicBoxes – Directi](#)

Domain Name:PRIVACYPROTECT.ORG
Created On:23-Sep-2004 11:55:58 UTC
Last Updated On:25-Aug-2008 10:53:22 UTC
Expiration Date:23-Sep-2009 11:55:58 UTC
Sponsoring Registrar: Directi Internet Solutions Pvt. Ltd. d/b/a PublicDomainRegistry.com

Registrant ID:PP-SP-001
Registrant Name: Domain Admin
Registrant Organization:PrivacyProtect.org
Registrant Street1:P.O. Box 97
Registrant Street2>Note - All Postal Mails Rejected, visit Privacyprotect.org
Registrant City: Moergestel
Registrant State/Province:
Registrant Postal Code:5066 ZH
Registrant Country: NL
Registrant Phone:+45.36946676
Registrant Email:contact@privacyprotect.org

PDR
(Directi)

PDR (Public Domain Registry) - They were #9 in the worst registrar report:
<http://www.knujon.com/registrars/> there are 14,096 spam-advertised PDR domains on record.
27% are software piracy
52% are fake pharmacy
17% are knockoff goods

ICANNWiki

Make A Donation

Go Search

article discussion edit history

Bhavin Turakhia

TOOLS ADD THIS



Bhavin is Founder, CEO and Chairman of [The Directi Group](#) (excerpt from website)

Bhavin brings over 12 years of technology experience and over 9 years of Market knowledge to the Directi Group and is today chiefly responsible for the Vision, Strategy, and Service Offerings of Directi. He has a very deep understanding of the Web Services Industry, a Strong Technical background, a keen Business sense, and most importantly, an unquenchable ambition for growth.

In 1998, at the age of 19, he founded Directi, with a focus to develop volume based Web Products and Services for a global audience. Directi is a technology-centric company, and an industry leading Web Services Provider serving a growing audience of Customers in 230 countries.

Bhavin is responsible for the vision and architecture of several Directi's Products and services. He has also been instrumental in defining, Directi's Corporate Structure and Business Process automation, which enable Directi to continue growing at triple digit growth rates year after year. He is a respected entity in the Web 2.0 landscape, and a frequent speaker at various seminars. He also serves as a technical advisor to the local CyberCrime Investigation Cell. He has won several awards, including the Entrepreneur of the year award in 2005.

Bhavin was also former chairman for the Global ICANN Accredited Registrars Constituency for two consecutive terms. He has been the youngest elected chair for this post in the history of ICANN. ICANN is the global Internet compliance and policy formation authority.

[Bhavin's Blog](#)

LOGICBOXES Registry & Registrar Solutions

resellerclub SKENZO WEBHOSTING.INFO

ICANNwiki: An industry resource fostering global collaboration and transparency within the ICANN community

Platinum Sponsors

SKENZO Traffic Monetization Solutions

LOGICBOXES Registry & Registrar Solutions

Gold Sponsors

Silver Sponsors

Bronze Sponsors

Fig 1.4 – Introduction to Directi, PDR (Public Domain Registry), Logic Boxes, Skenzo,

LogicBoxes
(Directi)

LogicBoxes are a major sponsor of ICANN (Internet Corporation for Assigned Names and Numbers), and part of Directi

Home Support

LOGICBOXES
Registry & Registrar Solutions

Home | About Us

Corporate Profile

About Us

- Corporate Profile
- Contact Us

LogicBoxes is a Software Development and Consulting Company with its primary focus on developing, deploying and managing Products, Services and Business Process Automation solutions for the Domain Registration and Web Hosting Industry. LogicBoxes is an industry leader in providing turn-key solutions for Domain Registrars, Web Hosts and Data Centers.

Our Product portfolio includes a comprehensive provisioning & management platform for various web Products/Services such as: Domain Registration, Windows/Linux Web Hosting, Email, SSL, Website Builder etc. LogicBoxes' Products/Services represent an R&D effort of over 8 years and in unison with OrderBox (the business automation module), form a comprehensive ERP solution for web service providers.

LogicBoxes currently powers the infrastructure and software of over 50 ICANN Accredited Domain Registrars including **Stargate, CI Host, EST Domains, ResellerClub, Expert Host** etc, several ccTLD Registrars and thousands of Web Hosts worldwide. We also provide Consultancy Services to Registrars, Registries and Web Service Providers. These services range from obtaining and managing ICANN/ccTLD Accreditations, to providing Business Process Automation and Outsourcing solutions.

Introduction | Hostex Overview | ICANN Accreditation Consultancy | ICANN Accreditation
About Us | Contact Us | News | Support | **Blog**
© 2008 LogicBoxes. All Rights Reserved.

Fig 1.5 – LogicBoxes corporate Profile – **Note: “Powers the infrastructure of EstDomains”**

LogicBoxes is still contractually obligated to provide software support and additional services to Estdomains, but Turakhia says he looks forward to the day when he can completely sever ties with Estdomains.

"I would really love to detach ourselves from that organization," he said. "We'll have to let portions of that contract run out on its own." - http://www.theregister.com/2008/09/03/directi_strikes_back/

Los Angeles 2007

SCHEDULE / AGENDA

MEETING MAP

PRESENTATIONS

TRANSCRIPTS

HELP

30th International Public ICANN Meeting, 29 October - 2 November 2007

Search

Welcome

SAT, 27 OCT | SUN, 28 OCT | MON, 29 OCT | TUE, 30 OCT | WED, 31 OCT | THU, 1 NOV | FRI, 2 NOV
| SAT, 3 NOV

DAILY CONFERENCE NEWSLETTERS



Photographs

There are a large number of pictures of the ICANN meeting and of the Gala event on Tuesday night. You will be able to review and purchase copies of these photos on the photographer's website here.



30th International Public
ICANN MEETING
Los Angeles 2007 29 Oct - 2 Nov



Welcome to Los Angeles

The City of Angels is ICANN's home town as well as the city that was in many ways the birthplace of the Internet. Taking place at the LAX Hilton hotel, the meeting represents a milestone for the organisation as well as a unique opportunity for the world's Internet community to gather together.

Navigation

- Venue / Hotels
- Agenda/Schedule
- Daily newsletters
- Social events
- Attractions
- Press
- Safety & Security
- About ICANN
- Content
- Recent posts
- Help
- Search

Log in

Visit Our Sponsors:



Fig 1.6 – LogicBoxes – Sponsorship of 30th ICANN meeting – LA USA 2007

Internet Influence

No inference is made or should be made as to wrongdoing by the following examples. They are shown to demonstrate the wider Internet connectivity that Atrivo requires

The Planet Internet Services

“The Planet is the worldwide leader in IT Hosting. Ranging from dedicated servers to enterprise-class managed hosting. We serve more than 22,000 customers from six SAS 70 Type II certified data centers. By providing world-class networking, the latest technologies and expert support, we enable our customers to successfully grow their businesses.”

- 1,546 of the PrivacyProtect sites are Planet sponsored.
- Hosting 3,166 infected web sites May 2008

ICANN

ICANN is the IP number assigning authority in the world. "ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet." icann.org/about/

Perhaps the most interesting claim by the various communications and in corporate information at the various noted websites, is the emphasis on being “ICANN accredited” and “carefully drawn up anti-abuse policies of ICANN” Unfortunately ICANN's anti-abuse policy is virtually nonexistent, in fact ICANN's 'official' statement shows:-

"If your complaint is about SPAM or computer viruses. The existence of SPAM and computer viruses are beyond the scope and authority of ICANN to resolve. If the content is of an illegal nature, or if you believe you are being spammed in violation of the law, you may wish to consult an attorney or an appropriate consumer protection agency. For further information about SPAM and tips to avoid "phishing" scams, you may wish to visit the U.S. Federal Trade Commission's SPAM website or Wikipedia"

However there is one area even ICANN is obliged to at least consider;

GAO (US Government Accounting Office) - requested - determine the prevalence of patently false or incomplete contact data in the 'Whois' service for the .com, .org, and .net domains; Based on a survey GAO concluded that 2.31 million domain names (5.14%) were registered with patently false data (data that appeared obviously and intentionally false) in one of more of the required contact information fields. So clearly there is contravention within this area of ICANN policy.

LogicBoxes and Skenzo host a "Taj Mahal Sojourn" for guests at the 31st ICANN Meet in Delhi, India

LogicBoxes and Skenzo host a "Taj Mahal Sojourn" for guests at the 31st ICANN Meet in Delhi, India

February 21, 2008, 03:04 AM

Apart from supporting the ICANN meet as silver sponsors, LogicBoxes and Skenzo planned this special event for as many as 90 attendees that had made the long trip to India. Arrangements were made for all guests to explore the mystical city of Agra and experience one of the Seven Wonders of the World – The Taj Mahal.

The elite list of attendees included the likes of Enom and Tucows head honchos, Paul Stahura and Elliott Noss respectively. Trey Harvin - CEO dotMobi, Jonathan Nevett - Network Solutions, Alexa Raad CEO PIR, Tim Cole - Chief Registrar Liaison at ICANN, Craig Schwartz - Chief gTLD Registry Liaison at ICANN, Tina Dam - Director, IDN Program ICANN, Dave Wodelet, Wendy Seltzer, Thomas Narten – ICANN Board members, and Chuck Gomes from Verisign just to name a few.

"It seemed like the perfect highlight for the 1st ever ICANN meet in India. We wanted our guests to experience the beauty of one of the most remarkable monuments in the world – the Taj Mahal! Since most had a busy agenda packed with meetings and discussions, this trip allowed the delegates to socialize and network while participating in this 'once in a life-time experience' " says Bhavin Turakhia, the CEO of Directi.

The trip included a comfortable drive in a convoy of luxurious coaches down the picturesque Golden Triangle of North India, followed by an awe striking tour of the Taj Mahal, a sumptuous lunch at the Mughal Sheraton coupled with a visit to other famous landmarks in Agra - a tour of the Agra Fort by the river Yamuna and the exotic Palaces within, some of the best specimens of Mughal art in India. And for all those who were looking at capturing the Indian culture in trinkets and artifacts, a trip was made to the local Bazaars that offered a wide choice of handicrafts, marble artwork, brassware, rugs, leather items and textiles etc.

The Taj Mahal Sojourn was a huge success being attended by several ICANN staff and Board members, Domain name Registry members and Registrars from across the globe. All those who joined the trip were enthralled by the magnificence of the monument and were able to explore and experience the culture and beauty of India in a different light.

"LogicBoxes and Skenzo have been associated with almost all ICANN meets for the past 3 - 4 years, and every year we try doing something different and innovative. The Taj trip certainly left our guests with memories that they will cherish forever! We wanted to give them a little something to take back, and nothing could be more memorable than a trip to the Taj Mahal." said Divyank Turakhia, President, Skenzo.

Skenzo's domain monetization program is used by a large number of ICANN Accredited Domain Registrars and several large domain portfolio holders to monetize their internet traffic. Despite its recent entry into the market, Skenzo has overtaken several other players to rank as the fastest growing company within the monetization market.

LogicBoxes is a software and consultancy company for Web Service Providers, Web Hosts and Registrars. Its software powers the backend of over 50+ ICANN Accredited Registrars, over 45000 Resellers and thousands of Web Service Providers worldwide.

Fig 1.6 – LogicBoxes Sponsorship of 31st ICANN meeting Feb 2008 – **Note: the elite list attending**

Level 3 Communications, Inc. (NASDAQ: LVT), an international communications company, operates one of the largest Internet backbones in the world, connecting 180 markets in 18 countries. The company serves a broad range of wholesale, enterprise and content customers, owner of Broadwing.

Atrivo - Hosted Infected sites

To provide quantification of the problem in direct and comparative terms, this section shows:

1. Fig 1.4 shows the number of infected sites hosted and served by Atrivo from November 2007 to July 2008. It further provides a percentage of infected web sites compared to the total of IP addresses. As a comparison an average percentage for web hosts would be around 0.01%

Note: Data courtesy of StopBadware.org, based on data provided by Google

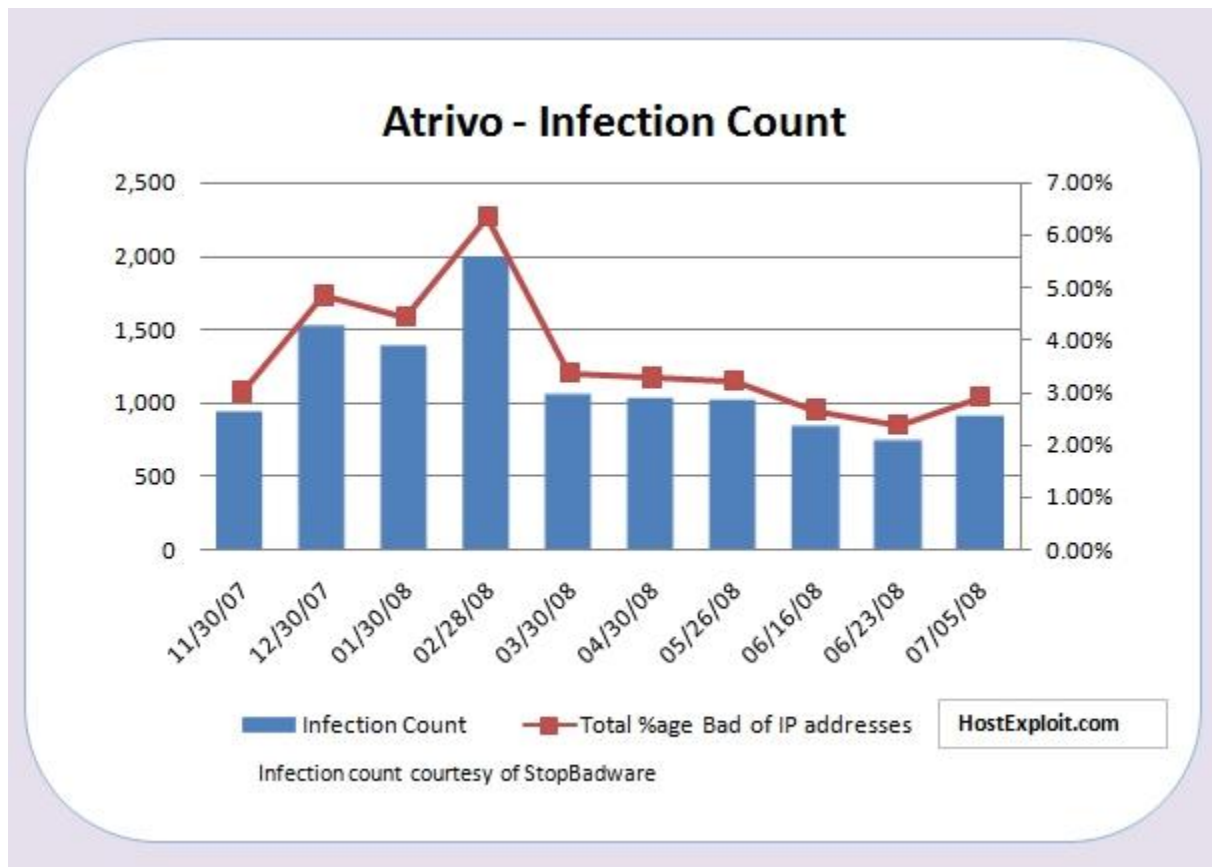


Figure 1.4 – Atrivo: Infected Web Sites – Nov 07 to July 08

2. Tables 1.1 provide a comparison of servers and hosts based on StopBadware's report on infected web sites / bad sites worldwide and comparing February 2008 with May 2008
 - (a) Shows the table based upon the highest number of infected web sites per AS number

(b) Shows the table based upon the added analysis of the number of infected sites per IP address. (note: this method establishes Atrivo at 4th worst worldwide)

3. Tables 1.2 provides a comparison of Atrivo, with servers directly controlled by Atrivo and Servers (AS) observed to be associated with Atrivo

asn	as_name	Country	Feb-08	May-08	% change	# IP addresses	# of infected sites / IP address
			infections	infections			
4134	CHINANET-BACKBONE No.31,Jin-rong Street	China	69,417	48,834	-29.65%	55,651,072	0.0009
4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	China	24,328	17,713	-27.19%	26,475,264	0.0007
4812	CHINANET-SH-AP China Telecom (Group)	China	14,157	9,445	-33.28%	4,739,840	0.0020
15169	GOOGLE - Google Inc.	USA	10,123	4,261	-57.91%	144,128	0.0296
9929	CNCNET-CN China Netcom Corp.	China	8,089	6,058	-25.11%	776,960	0.0078
17964	DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.	China	6,833	3,604	-47.26%	1,623,552	0.0022
21844	THEPLANET-AS - THE PLANET	USA	3,421	3,166	-7.45%	1,073,920	0.0029
36351	SOFTLAYER – SoftLayer Technologies Inc.	USA		3,507		276,480	0.0127
29629	INetwork-AS IEUROP AS	France		2,878		8,192	0.3513
37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology Co., Ltd	China	2,604			4,096	0.6357
24400	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.	China	2,515			59,392	0.0423
4538	ERX-CERNET-BKB China Education and Research Network Center	China	2,455			12,835,584	0.0002
17816	CHINA169-GZ CNCGROUP IP network China169 Guangzhou MAN	China	2,378			1,458,944	0.0016
23724	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation	China	2,181	2,357	8.07%	170,496	0.0138
36420	EVERYONES-INTERNET3 - Everyones Internet	USA	2,148			119,552	0.0180
4808	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network	China	2,049			3,540,224	0.0006
27595	ATRIVO	USA		1,007		31,232	0.0322

Table 1.1 (a) The top networks hosting badware websites - based on number of infections

asn	as_name	Country	Feb-08	May-08	% change	# IP addresses	# of infected sites / IP address
			infections	infections			
37943	CNNIC-GIANT ZhengZhou GIANT Computer Network Technology Co., Ltd	China	2,604			4,096	0.6357
29629	INetwork-AS IEUROP AS	France		2,878		8,192	0.3513
24400	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.	China	2,515			59,392	0.0423
27595	ATRIVO	USA		1,007		31,232	0.0322
15169	GOOGLE - Google Inc.	USA	10,123	4,261	-57.91%	144,128	0.0296
36420	EVERYONES-INTERNET3 - Everyones Internet	USA	2,148			119,552	0.0180
23724	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation	China	2,181	2,357	8.07%	170,496	0.0138
36351	SOFTLAYER – SoftLayer Technologies Inc.	USA		3,507		276,480	0.0127
9929	CNCNET-CN China Netcom Corp.	China	8,089	6,058	-25.11%	776,960	0.0078
21844	THEPLANET-AS - THE PLANET	USA	3,421	3,166	-7.45%	1,073,920	0.0029
17964	DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.	China	6,833	3,604	-47.26%	1,623,552	0.0022
4812	CHINANET-SH-AP China Telecom (Group)	China	14,157	9,445	-33.28%	4,739,840	0.0020
17816	CHINA169-GZ CNCGROUP IP network China169 Guangzhou MAN	China	2,378			1,458,944	0.0016
4134	CHINANET-BACKBONE No.31,Jin-rong Street	China	69,417	48,834	-29.65%	55,651,072	0.0009
4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	China	24,328	17,713	-27.19%	26,475,264	0.0007
4808	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network	China	2,049			3,540,224	0.0006
4538	ERX-CERNET-BKB China Education and Research Network Center	China	2,455			12,835,584	0.0002

Table 1.1 (b) The top networks hosting badware websites - based on number of infected sites per IP address

Table 1.1 - The top network (AS) blocks hosting badware websites - courtesy of StopBadware - analysis HostExploit.com

asn	as_name	Country	infections Apr 08	# IP addresses	# of infected sites / IP address
27595	ATRIVO (also Interage, Hostfresh, EstHost, EstDomains)	USA	1,023	31,232	0.0328
(i) Attrivo - directly controlled /managed:					
36445	CERNEL (Also Interage)	USA	8	4,864	0.0016
26769	BANDCON	USA	553	12,544	0.0441
3356	BROADWING (Interage custom blocks / racks)	USA	176	210,176	0.0008
(ii) Attrivo - associated / AS blocks observed to receive and connect to exploit sites					
36351	SOFTLAYER	USA	3,325	276,480	0.0120
9121	TTNET TNet Autonomous System	TK	533	5,916,928	0.0001
30968	INFOBOX	RU	133	276,480	0.0005
29131	RAPIDSWITCH-AS RapidSwitch Ltd	UK	82	16,384	0.0050
41947	WEBALTA	RU	107	55,296	0.0019
4657	STARHUB	SG	51	26,112	0.0020
44394	BUILDHOUSE-AS Buildhouse Ltd.	RU?	12	4,864	0.0025
26627	PILOSOFT	USA	41	68,096	0.0006
19151	WVFIBER	USA	8	273,664	0.0000
32959	LITEUP	USA	6	66,048	0.0001
4436	NLAYER	USA	1	5,916,928	0.0000
			<u>6,059</u>		

Table 1.2 (a) Data courtesy of StopBadware based on data provided by Google Analysis: HostExploit.com

asn	as_name	feb	mar	apr	may	jun	jul
27595	ATRIVO (also Interage, Hostfresh, EstHost, EstDomains)	1,981	1,048	1,023	1,007	831	910
(i) Attrivo - directly controlled /managed:							
36445	CERNEL (Also Interage)	0	6	8	8	8	17
26769	BANDCON	1,935	0	553	0	0	0
6395	BROADWING (Interage custom blocks / racks)	130	137	176	155	107	134
(ii) Attrivo - associated / AS blocks observed to receive and connect to exploit sites							
36351	SOFTLAYER	1,812	2,622	3,325	3,507	1,607	1,520
9121	TTNET TNet Autonomous System	217	472	533	434	316	301
30968	INFOBOX	308	150	133	136	100	86
29131	RAPIDSWITCH-AS RapidSwitch Ltd	32	69	82	133	62	65
41947	WEBALTA	103	108	107	89	80	64
4657	STARHUB	39	50	51	37	22	33
44394	BUILDHOUSE-AS Buildhouse Ltd.	4	9	12	15	15	28
26627	PILOSOFT	51	46	41	40	20	23
19151	WVFIBER	6	6	8	4	1	15
32959	LITEUP	0	8	6	4	1	2
4436	NLAYER	13	1	1	2	2	2
		<u>6,631</u>	<u>4,732</u>	<u>6,059</u>	<u>5,571</u>	<u>3,172</u>	<u>3,200</u>

Table 1.2 (b) Data courtesy of StopBadware based on data provided by Google Analysis: HostExploit.com

Section 2: Atrivo – Exploitation a Case Study

This case study is a real example of how exploitation of an end user works. Figure 3 below provides a diagrammatic over view to show the steps and interaction, an educational video is also available on You Tube

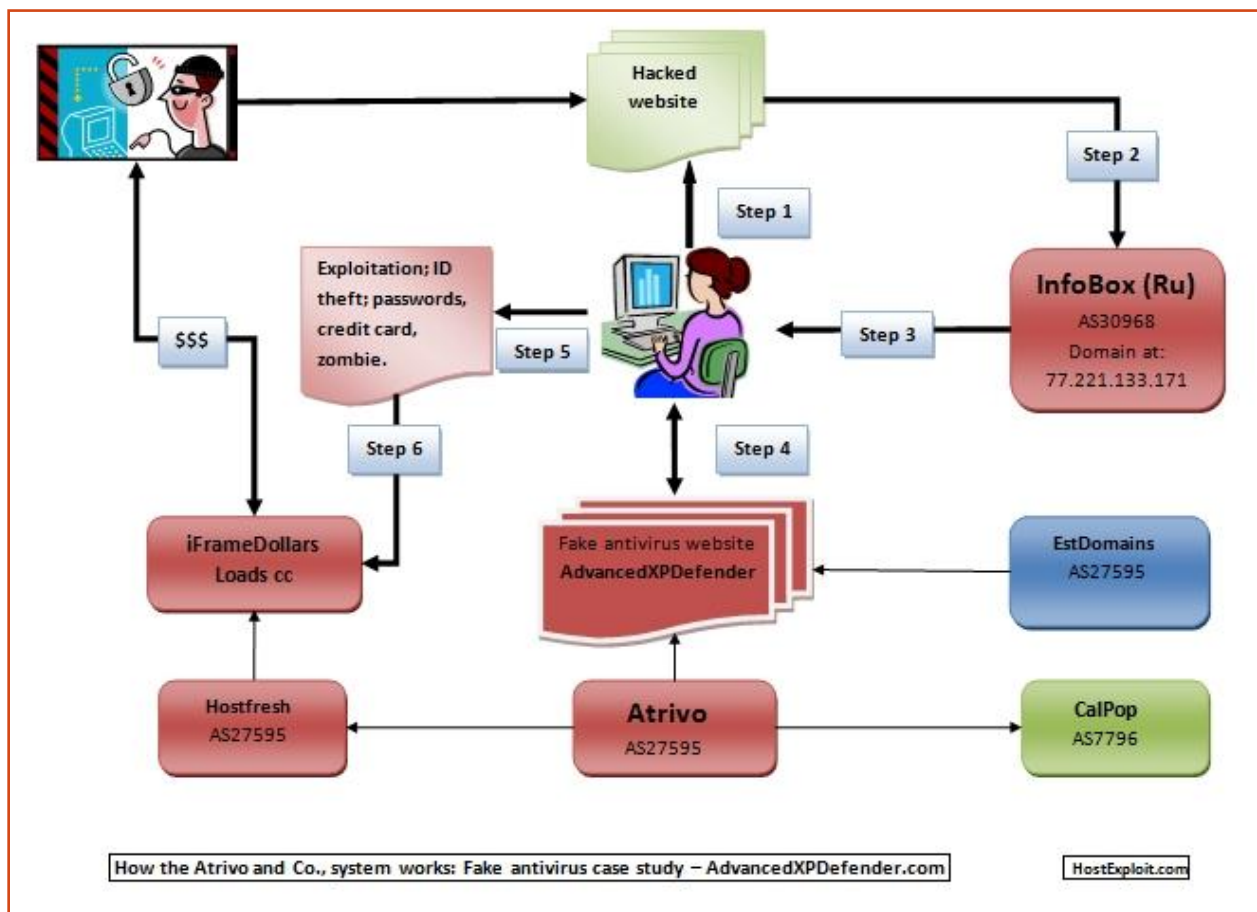


Figure 2.1

Figure 2.1 - provides a recent and specific example of exploitation of a PC user



Initially, hackers break into a server hosting a legitimate web site. They erase logs which document the break in, so as to not alert the server's owner. The hackers install a back door to enable ease of reentry or install a program which transmits credit card and other sensitive information back to them. They also install a hidden JavaScript program which will redirect web site visitors to a malicious web site.

Web site is hacked through any number of different methods.

- Actual web server is breeched
- FTP login information acquired from malevolent means.
- User installed applications on the web server with vulnerabilities that allow access to hackers.
- Server applications with vulnerabilities allow access to hackers.
- Email notice to web user with Malware attachment

Hackers are able to break into web servers due to weak passwords, improperly configured server settings, un-patched operating systems, insecure program code, compromising an administrator's workstation, and by exploiting vulnerabilities that software vendors have yet to provide a patch for.

The PC user -- how they get infected

Step 1

In Step 1, a home PC user visits a trusted and familiar web site on the hacked server.

Step 2

When visiting the hacked site, the visitor is redirected to the fake Antivirus site on a InfoBox or other Malware server. This fake antivirus site generates high confidence levels to the visitor by displaying several well known "sponsored by" or affiliate logos. Other means of stealing information can include "drive-by downloads" where due to the hacked site a Trojan or worm is installed in the user's PC completely without intervention by the user and is often undetected by traditional spy-war and antivirus programs.

Step 3

A very prominent and urgent message is displayed on the visitors screen stating their computer is infected with a serious virus, Trojan or worm. "The user is then prompted to pay for a full license of the application in order to remove the errors.

Step 4

During Step 4, the fake anti-virus web site displays high production values and appears legitimate. It generates positive confidence levels to the visitor by displaying several well known "sponsored by" or

affiliate logos. The fake antivirus program, "AdvancedXPDefender" (or any of a number of other fake antivirus program names) launches a fake online scan. The online scan is an attempt to install a Trojan on the user's PC. If the home user's PC has an un-patched operating system, the computer becomes infected.

Step 5 During Step 5 the fake anti-virus software reports that the user's computer is infected with a specific virus; it may be a virus that the user has heard of previously. The home user is prompted to purchase and download the fake anti-virus software so that the (non-existent) virus can be removed. If the home user downloads the fake anti-virus software, their computer becomes infected (even if its operating system is patched). If the home user has anti-virus software installed, the fake anti-virus software disables it. If the user purchases the fake anti-virus software, their credit card and personal identity information are stolen.

Step 6 In Step 6, the stolen information of the home user is uploaded to the iFrameDollars website and is subsequently sold to others who exploit stolen identities. At the loads.cc web site, the data feeds being transmitted by the virus on the home user's PC are sold in bulk to cyber criminals who create botnets with infected computers, etc.



\$\$\$ iFrameDollars sells stolen ID's and credit card information to other hackers and cyber criminals for the sole purpose of exploiting the original web site visitor.

\$\$\$ Loads.cc - charge cyber criminals for infected PCs. on botnets, the size of which is estimated to be a few million, and infect PCs with whatever malware they choose for a little fee. Currently, loads.cc claims to have 264,552 hacked systems in more than a dozen countries that it can use as hosts for any malicious software that clients want to install. The latest details from the "statistics" page displayed for members says the service has gained some 1,679 new infected nodes in the last two hours, and more than 33,000 in any 24 hour period.



The different forms of exploitation

Now that the Malware vendor has obtained the web visitors private information, ID Theft occurs



Rogues and Fakes



Advanced XP Defender

Click here to perform a FREE Spyware scan

Overview | Download | Company | Features | Updates | Support

91% of home PCs are Infected!

Advanced XP Defender is a powerful mix of Anti-Malware, Anti-Virus, Anti-Trojan, Anti-Backdoor, Anti-Worm and Anti-PomoDial in one program. It will protect you from all types of Viruses on your PC.

Download | Buy Now! | Features

Information

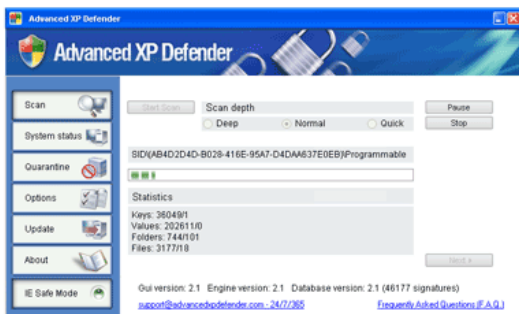
Statistics approve that virus and trojan attacks damage more than \$3 million/hour and the new virus appears each hour. One of them, virus Sasser. A, infected million of computers at the first hours after let out and caused billions damages. It had been corrected within a lot of months.

Advanced XP Defender key features

Full Windows XP Service Pack 2 Security Center Support!

RescueScan Technology - With Ultra-high speed scan rescuing yours PC from Viruses for few seconds!

Ultimate Live Update - Each 2 hours anti-virus bases and modules are completely updated. Advanced XP Defender stands sentinel over your privacy and identity!



- Advanced XP Defender finds out and removes more than 100000 Trojan horses, Spyware, Viruses, Hackers, Adware, Keyloggers and another harmware;
- Advanced XP Defender allows scan files quickly and access other features Advanced XP Defender directly from Windows Explorer;
- Removes "active trojan" from a disk even if it is blocking the file;
- Removes trojan files are locked for writing (for example .DLLs being used);
- Best backdoor and worm protection;
- Supports compressed files scan;
- Reports and Activity Log functionality;
- Virus Removal Assistant can force clean the stubborn trojans and spyware than the other removal tools cannot;
- The Behavior Analysis Technology can find out the unknown trojans and spyware better;
- The scheduled scan supports automatic scan at specified time;
- Lowest CPU usage rate, best performance and modern user GUI.

(NBW) Advanced XP Defender is a powerful and simple in use Trojan horses, Viruses and all types of Malware removal software for detects and eliminates more than 100'000 Trojan Horses and Spywares. Viruses, trojans, worms, spyware, malicious ActiveX

The realistic look of the Rogue PC security web site

Domain Name: ADVANCEDXPDEFENDER.COM - Registrar: **ESTDOMAINS, INC.**

Whois Server: whois.estdomains.com

Name Server: NS1.ADVANCEDXPDEFENDER.COM

Name Server: NS2.ADVANCEDXPDEFENDER.COM

Updated Date: 07-may-2008, Creation Date: 07-may-2008, Expiration Date: 07-may-2009



Reported Attack Site!

This web site at advancedxpdefender.com has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#)

[Why was this site blocked?](#)

[Ignore this warning](#)

Safe Browsing

Diagnostic page for advancedxpdefender.com/

Advisory provided by [Google](#)

What is the current listing status for advancedxpdefender.com/?

Site is listed as suspicious - visiting this web site may harm your computer.

Part of this site was listed for suspicious activity 2 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 21 pages we tested on the site over the past 90 days, 1 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 06/22/2008, and the last time suspicious content was found on this site was on 06/09/2008.

Malicious software includes 1603 trojan(s). Successful infection resulted in an average of 3 new processes on the target machine.

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, advancedxpdefender.com/ did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?

Yes, this site has hosted malicious software over the past 90 days. It infected 3351 domain(s), including 77.221.133.0, sporkolej.com, junkinside.com.

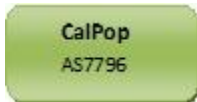
How did this happen?

In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

Next steps:

- [Return to the previous page.](#)
- If you are the owner of this web site, you can request a review of your site using Google [Webmaster Tools](#). More information about the review process is available in Google's [Webmaster Help Center](#).

©2008 Google - [Google Home](#)



The commercial rack space rented by Atrivo

CalPOP.com, Inc.
600 W. 7th St. Third Floor
Los Angeles, CA 90017
(213) 627-7927 Voice
(213) 627-2912 Fax

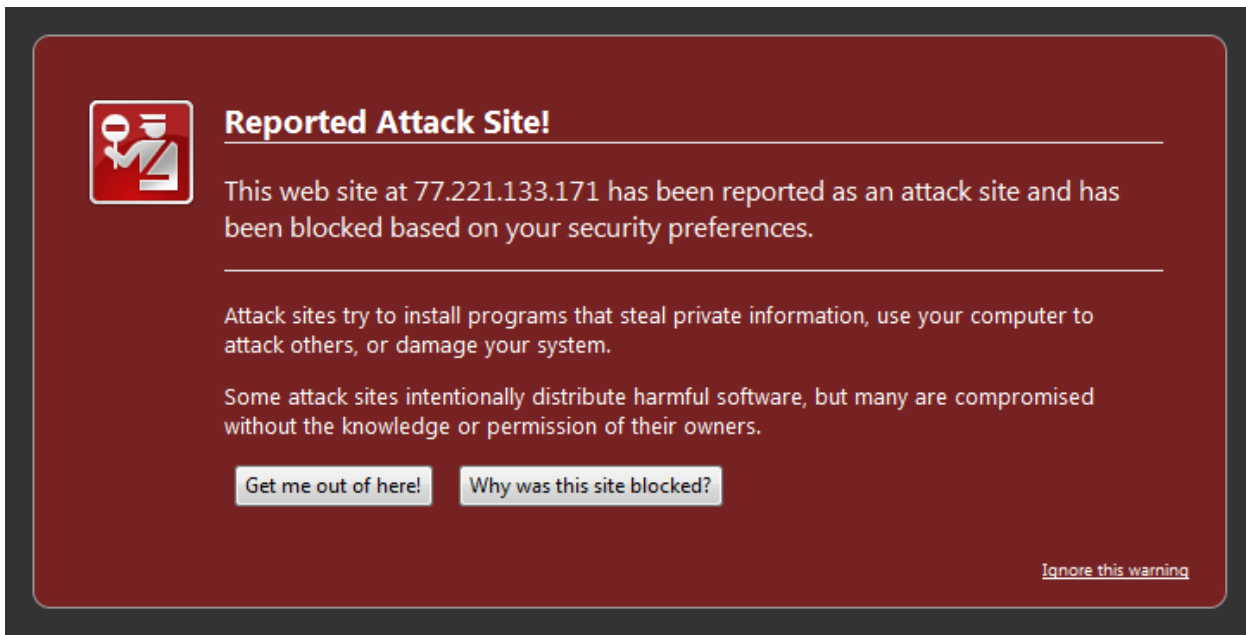
Call Now We're Always Open!
1-855-467-8846
FREE 24 Hour On-Site Support!

CalPOP is connected throughout the world via OC192 internet backbone fiber. CalPOP has over 10,000 square feet of Data Center space in Downtown Los Angeles with where it hosts thousands and thousands of servers and hundreds and hundreds of data cabinets. CalPOP operates several networks and interconnects networks via BGP4 via JUNIPER routers. CalPOP is carrier neutral but CalPOP also offers true multi-homed gigabit connectivity with separate Cogent and at 10 Gigabit connections to Level3, Savvis, Sprint, Cogent, AT&T, and SOX. CalPOP has fiber to the P&O and EQC/ENJ peering fabrics and is located at 600 W. 7th Street in Downtown Los Angeles. This is where AS6, peering to LA and where you can cross connect to nearly any provider. CalPOP offers both quality network connectivity with greater peering and also offers low cost and reliable network connectivity. CalPOP's high connectivity ensures the fastest network speed available!

Microsoft | CentOS | Ubuntu | CISCO | Red Hat | HP | Intel | MySQL | iPanel | AMD | Debian

InfoBox (Ru)
AS30968
Domain at
77.221.133.171

The exploit server – Google’s safe browsing Safe Browsing Diagnostic page for 77.221.133.171



Reported Attack Site!

This web site at 77.221.133.171 has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#) [Why was this site blocked?](#)

[Ignore this warning](#)



The hacker at work



DANGEROUS: LinkScanner Online has found [Rogue spyware scanner]

Detail: Exploit: Rogue Spyware Scanner

This is probably a pitch-page for one of the many rogue spyware programs.

Risk Category: Exploit

Description: XPL's Intelligence Network has detected an exploit. An exploit is a piece of malware code that takes advantage of vulnerability in a software application, usually the operating system or a web browser to infect a computer. Exploits usually target a computer by means of a drive-by download – the user has no idea that a download has even taken place. XPL recommends not visiting this web site regardless if your computer has been patched for the vulnerability.

Scanned: Monday, June 23, 2008

Our Advice: **This page contains at least one exploit. You should not click on this link without appropriate anti-exploit protection on your PC.** If you'd like to have the power of LinkScanner Online automatically available to you whenever you're on the web, download a free trial version of LinkScanner Pro now. LinkScanner Pro provides constant protection against infection from rapidly-changing malicious websites and exploits without the need to manually run LinkScanner on every site you want to visit.



DANGEROUS: LinkScanner Online has found [Rogue spyware scanner]

Detail: Exploit: Trojan installer

This is code that is used to trick victims into installing potentially unwanted software.

Risk Category: Exploit

Description: XPL's Intelligence Network has detected an exploit. An exploit is a piece of malware code that takes advantage of vulnerability in a software application, usually the operating system or a web browser to infect a computer. Exploits usually target a computer by means of a drive-by download – the user has no idea that a download has even taken place. XPL recommends not visiting this web site regardless if your computer has been patched for the vulnerability.

Scanned: Monday, June 23, 2008

Specific References:

(1) April 28th, 2008

Developers at fault? SQL Injection attacks lead to wide-spread compromise of IIS servers

<http://blogs.zdnet.com/security/?p=1059>

(2) Sunday July 27, 2008

[Beware Fake Malware Cleaner Programs](#)

http://blogs.pcmag.com/securitywatch/2008/07/beware_fake_malware_cleaner_pr.php

(3) Jul24, 2008

Fake Trend Micro Virus Clean Tool Spreads Malware Dirt

<http://blog.trendmicro.com/fake-trend-micro-virus-clean-tool-spreads-malware-dirt/>

(4) New Spyware (Wrongly) Claims It's Won PCMag Award

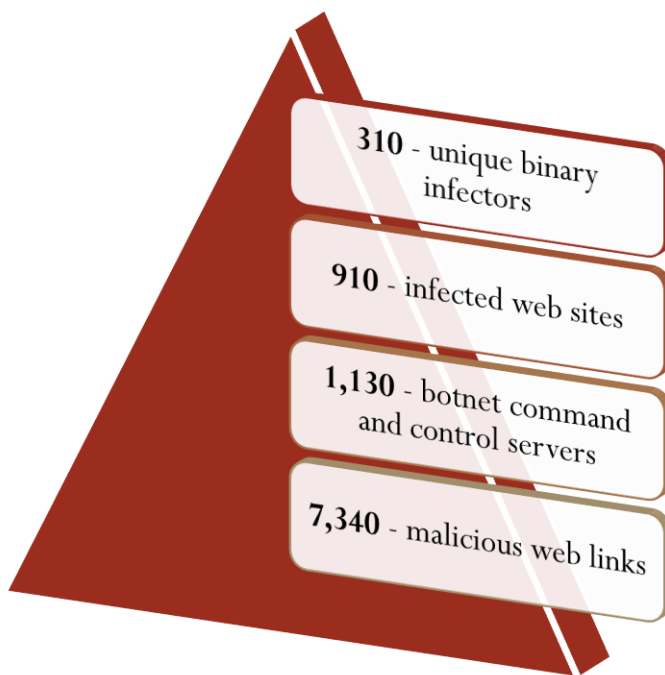
http://news.yahoo.com/s/zd/20080722/tc_zd/230062

(5) Sunday July 13, 2008

Identities For Sale! \$1 Apiece!

http://blogs.pcmag.com/securitywatch/2008/07/identities_for_sale_1_apiece.php

Section 3: Atrivo – Results and Analysis



Atrivo - The Hierarchy of Exploitation - Figure 3.1

Analysis was made of the IP space associated with, leased to or by Atrivo & Intercage & Co., from various methods and community sources. Note: many of the technical terms are explained within 'Appendix 2 – Glossary of Terms'. The highlights of the discoveries were from 26,000 Atrivo domains:

(a) Figure # represents an extrapolation of **10%** random sampling of known Atrivo IP addresses (**2,600**) that resolve to the Atrivo IP space was selected (**26,000**). Each of these domains was visited by an automated tool that downloads all content from each domain and follows one link further. This showed:

310 binaries - 31 files retrieved from Atrivo domains were analyzed from the 10% sample, and all 31 of these were known malware. Each sample was run through a 'sandnet', each was deemed hostile and tried to deliver information to or receive commands from Atrivo IP or related space.

Note: each of these 31 files was linked to many web sites. As seen previously, the Russian Business Network (RBN), their affiliates and other organized crime groups have sought to realize economies of scale in the delivery of malware. Limiting the actual number of malicious binaries in a given IP address range also provides a degree of stealth from Internet malware scanners such as McAfee's Site Advisor.

910 infected web sites - Sites that are identified by 'StopBadware' as exhibiting badware behavior may be deliberately participating in the distribution of malware or may be compromised through manual or automated means. This does not distinguish among sites based on intent, but rather treats all of the sites equally as vectors for malware infection. (3)

1,130 botnet C&C controllers - 113 botnet C&C (command and control) servers were identified from the 10% Atrivo IP space analysis.

7,340 malicious web links - minimum of 734 links to fake and/or malicious security products in the sample of 2600 domains. Any porn sites were excluded from within the 10% sample (see below).

(b) As noted regularly by Sunbelt and many other sources (4) (5) Atrivo is also the main source on the Internet for 'rogue anti-virus and fake codecs'. Figure 2 demonstrates this for an individual user, Figure 3 below shows the servers and hosts for the top 100 of the rogues and fakes.

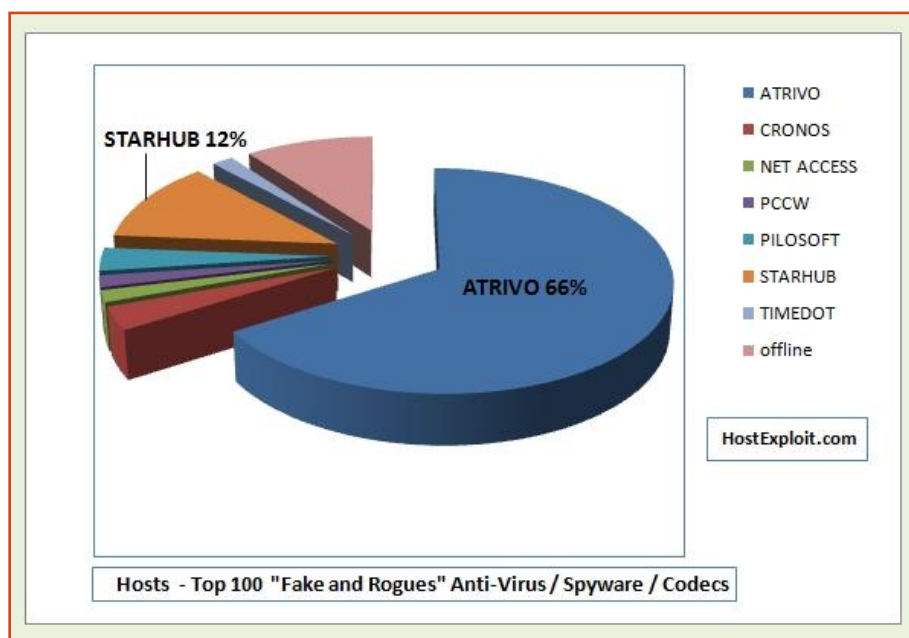


Figure 3.1

(c) 78% of evaluated Atrivo domains and mail servers are rated hostile (based upon 465 random domains via WOT (Web of Trust) (6)

(d) 145 fake porn site redirectors, were also detected which use a DNS changer – based on the 'MovieCommander' DNS hijacking malware rootkit. The effect of which alters the PC users router and web surfing. (6) (7).

It should be further noted some of the adult sites hosted are either border line or are within known blacklists of pedo-pornographic web sites (Note: this topic is outside the remit of this study, however details have been passed to appropriate third parties).

(e) The table 3.2 below provides a breakdown of the various Atrivo IP ranges and interpreted badness served and distributed.

Server	IP Range	No. Of IP Addresses	Interpreted Badness Served & Activity Observed During 2008	Server Types
HOSTFRESH	58.65.238.1 to 58.65.238.254	254	Served the feebos trojan as an integral part of the massive I-frames injection attacks against CNet, History.com, TorrentReactor, and Wired.com. Includes fake Western Union, Google and rogue security software web sites as well as, spam servers.	Exim on Debian like servers
HOSTFRESH	58.65.239.1 to 58.65.239.254	254	Fake AT&T, Google and fax monitoring sites, financial scam sites, and porn sites.	Exim on Debian like servers
CERNEL	64.28.176.1 to 64.28.191.254	4,094	Includes a portfolio of fake video codec (Zlob trojan), and DNS hijacker sites, fake mp3 download sites, fake security softwaresites, online pharmacy sites, malicious and porn redirects , spam servers.	Postfix and Sendmail on Linux distros.
CERNEL	67.210.0.1 to 67.210.7.254	2,046	Including various fast flux and revolving DNS and web servers.	Unix and Microsoft operating systems.
CERNEL-ESTHOST	67.210.13.1 to 67.210.13.254	254	Targeting gamers and Harry Potter fans. Also includes gambling and scam real estate sites.	CentOS and Fedora operating systems.
CERNEL-ESTHOST	67.210.14.1 to 67.210.15.254	510	Online pharmaceuticals, high yield investment programs, porn, and distributed denial of service reselling.	CentOS and Fedora operating systems.
CERNEL	67.210.8.1 to 67.210.11.254	1,022	Including various fast flux and revolving DNS and web servers.	Unix and Microsoft operating systems.
NLAYER-BROADWING	69.22.162.1 to 69.22.163.254	510	Gambling, scam realty (focusing on Caribbean and Dominican properties), scam ticket sales, and a site targeting cancer patients.	Unix servers.
NLAYER-BROADWING	69.22.168.1 to 69.22.175.254	2,046	Pakistan and Toronto-based (da.fedz.are.tryin.to.g3t.us, nobody.has.teh.ballz.to.f1ght.us) hackers. Includes sites targeting children (cartoon-classics.com, gamehosts.com), phishing (gorockfish.net)	Unix servers.
NLAYER-BROADWING	69.22.184.1 to 69.22.187.254	1,022	Hosting apparent pedoporn	CentOS and Unix.
NLAYER-BROADWING	69.31.64.1 to 69.31.79.254	4,094	Used by Toronto based hackers (i.m.a.soldier.pr0.us, currupt.federal-agency.net, uses.a.secure.eggdrop-hosting.biz), ESTHOST and various porn sites .	Debian, FreeBSD, Unix.
BROADWING-INTERCAGE	69.50.160.1 to 69.50.191.254	8,190	Leased by InterCage, Inc. IFRAME trojan injection attacks against (CNet, Wired.com and History.com). Hosting for apparent pedoporn, fake security software sites (adwarecleaner.net, allspyremover.net, cleanyourpc.net). Scam casino and dating sites engage in identity theft. ESTHOST & ESTDOMAINS is present.	FreeBSD and Unix OSs, and Sendmail - spam.
CERNEL-UKRTELEGROUP	85.255.113.1 to 85.255.121.254	2,286	Includes sites hosting the DNS changer trojan which targeted Mac and Windows. Hosting services for pedoporn, fake security software and financial crime sites. Heavily infested with viruses and other malware.	Unix and Linux OSs.
HOSTFRESH	116.50.10.1 to 116.50.10.254	254	Flux botnet and revolving DNS servers.	CentOS.
HOSTFRESH	116.50.11.1 to 116.50.11.254	254	Flux botnet and revolving DNS servers.	CentOS.
INTERCAGE	216.255.176.1 to 216.255.191.254	4,094	Participated in iframe injection attacks USAToday.com, ABCNews.com, News.com, Target.com, Walmart.com, Sears.com, Forbes.com, etc. Est Host - pornographic cartoon sites. varieties of typosquatter, and scam sites infect visitors. Estdomains	Unix OSs. Sendmail and Postfix - spam

31,184

HostExploit.com 2008

Table 3.2 - Atrivo IP Ranges and Badness Served

Section 4: Atrivo – Conclusions and Actions

This study even in this ‘lite’ format clearly shows why we coined the title ‘Atrivo – Cyber Crime USA’ As stated earlier the Internet community has a choice either resolve these problems ourselves or risk losing the generative and freewheeling Internet we all enjoy.

It has to be understood the art form of analyzing cyber crime is similar to studying stage magicians or illusionists. Much effort is made to switch domains, malware, spam and badware on a regular basis between various AS and IP ranges in an attempt to confuse or obscure. Hence as shown we provide wider listings and observations of the various AS ranges and often associated servers. It would be naïve of us to believe the cyber criminals do not also investigate mechanisms and tools that are used to probe them.

Specific issues:

1. The average user wants and looks to gain a certain level of privacy on the Internet, and many fully support EFF’s (Electronic Frontier Foundation) stance. One of ICANN’s arguments for its inability or unwillingness to act against registrars who house cyber crime is that of European and/or US mandates on privacy. However, in our opinion, there is a clear difference between a blogger or Internet user reasonably seeking anonymity or not to be tracked, and the cyber criminal who wishes the same anonymity.
2. As clearly demonstrated, there are many organizations which are in some way linked or being charitable, are duped into the chain of cyber crime. Above we show as examples Level 3 Communications, The Planet and CalPop, there are also many others. The argument is well known; “Well we just sell; server / rack space / domains/ privacy, what the purchaser does with it is not our affair” — Ultimately there must be some level of business ethics that would say, “Perhaps we should examine our policies more closely and act in the interests of the public?” – It is clearly the case the Internet community has not yet demonstrated its requirements for ethical business decisions. Unfortunately there will be the occasion when a victim decides to seek legal redress for losses.
3. We have seen an earlier statement from Emil Kacperski on behalf of Atrivo stating – “We will shut down and take offline any servers that have malicious software or causing harm to anyone. But of course we need proof that this is the case.” – Well Emil we have the proof.

Actions:

As we have indicated this is a first ‘lite’ version with monthly updates to come. However we know it is not just us who want to ‘stop’ this, perhaps a good start will be to hear from The Planet, Level 3, CalPop and others. Perhaps the development of a widely circulated list of ‘ethical’ Internet servers, backbones, and Internet companies who are prepared to support the continuance of the ‘generative’ internet.

Appendix 1: Atrivo – Links, References, and Further Reading

HostExploit

<http://www.hostexploit.com/>

CyberDefcon

<http://www.cyberdefcon.com/>

Jart Armin

<http://www.jartarmin.com/>

RashBL

<http://www.rashbl.com/>

Knujon – specific re: Directi

<http://www.knujon.com/news.html#08282008> and

<http://www.knujon.com/news.html#directi>

Brian Krebs' Security Fix

<http://blog.washingtonpost.com/securityfix/>

CastleCops:

<http://www.castlecops.com/>

Cyber-TA Malware Analysis:

<http://www.cyber-ta.org/releases/malware-analysis/public/>

Cybercrime & Doing Time:

<http://garwarner.blogspot.com/>

Dancho Danchev:

<http://ddanchev.blogspot.com/>

Danger Room:

<http://blog.wired.com/defense/>

Digital Intelligence and Strategic Operations Group:

<http://www.disog.org/>

EmergingThreats.net:

<http://www.emergingthreats.net/>

Honeywall Samples:

<http://doc.emergingthreats.net/bin/view/Main/HoneywallSamples>

Jart Armin's RBN Exploit:

<http://rbnexploit.blogspot.com/>

Knujon

<http://knujon.com>

Malware Domains:

<http://malwaredomains.com/>

RBN IP listings:

<http://doc.emergingthreats.net/bin/view/Main/RussianBusinessNetwork>

SANS Internet Storm Center:

<http://isc.sans.org/>

SecureHomeNetwork:

<http://securehomenetwork.blogspot.com/>

Securiteam:

<http://blogs.securiteam.com/>

Shadowserver.org:

<http://www.shadowserver.org/wiki/>

Spamhaus.org:

http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=R0K7465

SpamHuntress – 2005 but just as relevant today

<http://spamhuntress.com/2005/09/04/atrivo-on-esthost/>

SRI Malware Threat Center:

<http://mtc.sri.com/>

StopBadware:

<http://stopbadware.org>

Sunbelt Blog:

<http://sunbeltblog.blogspot.com/>

Symantec Threat Explorer:

http://www.symantec.com/business/security_response/threatexplorer/threats.jsp

Team Cymru:

<http://www.cymru.com/>

URIBL – because spam sucks

http://rss.uribl.com/nic/ESTDOMAINS_INC_.html

Victor Julien's Inliniac:

<http://www.inliniac.net/blog/>

Will Metcalf's Blog:

<http://node5.blogspot.com/>

Rev 1.1. Update on Specific Report References – Selection

Washington Post – Brian Krebs

http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html

Spamhaus – Cybercrime's US Hosts

<http://www.spamhaus.org/news.lasso?article=636>

StopBadware

<http://blog.stopbadware.org/2008/08/28/report-calls-out-atrivo-intercage-and-affiliates>

The Register – Dan Goodin

http://www.theregister.com/2008/09/03/cyber_crime_reports/

HostsNews – Intercage Suspends Thousands of Malware Sites

<http://msmvps.com/blogs/hostsnews/archive/2008/09/03/1646589.aspx>

Softpedia - <http://news.softpedia.com/news/Spam-at-the-Highest-Levels-92932.shtml>

Appendix 2: Glossary of Terms

Autonomous System/Server (AS): An AS is a unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of an entity (such as a university, a business enterprise, or ISP). An AS is also sometimes referred to as a routing domain. Each autonomous system is assigned a globally unique number called an Autonomous System Number (ASN).

Badware: Software that fundamentally disregards a user's choice regarding how his or her computer will be used. You may have heard of some types of badware, such as spyware, malware, or deceptive adware. Common examples of badware include free screensavers that surreptitiously generate advertisements, malicious web browser toolbars that take your browser to different pages than the ones you expect, or keylogger programs that can transmit your personal data to malicious parties.

Blacklists: In computing, a blacklist is a basic access control mechanism that allows access much like your ordinary nightclub; everyone is allowed in except people on the blacklist. The opposite of this is a whitelist, equivalent of your VIP nightclub, which means *allow nobody, except members of the white list*. As a sort of middle ground, a greylist contains entries that are temporarily blocked or temporarily allowed. Greylist items may be reviewed or further tested for inclusion in a blacklist or whitelist. Some communities and webmasters publish their blacklists for the use of the general public such as Spamhaus or Emerging Threats.

Botnet: Botnet is a jargon term for a collection of software robots, or bots, that run autonomously and automatically. The term is now mostly associated with malicious software where cyber criminals but it can also refer to the network of computers using distributed computing software.

DNS (Domain Name System): DNS associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. *www.example.com*, into IP addresses, e.g. *208.77.188.166*, which networking equipment needs to deliver information. A DNS also stores other information such as the list of mail servers that accept email for a given domain. By providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of contemporary Internet use.

Exploits: Turning the verb for taking advantage of a weakness into a noun, but with the same meaning, just in a digital sense, an exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause irregular behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as violently gaining control of a computer system or allowing privilege escalation or a denial of service attack.

Hosting: Usually refers to a computer (or a network of servers) that stores the files of a web site which has web server software running on it, connected to the Internet. Your site is then said to be hosted.

Malicious Links: These are links which are planted on a site to deliberately send a visitor to a malicious site, e.g. a site with which will plant viruses, spyware or any other type of malware on a computer such as a fake security system. These are not always obvious as they can be planted within a feature of the site or masked to misdirect the visitor.

MX: A mail server or computer/server rack which holds and can forward e-mail for a client.

Open Source Security: Open source is a set of principles and practices that promote access to the production and design process for various goods, products, resources and technical conclusions or advice. The term is most commonly applied to the source code of software that is made available to the general public with relaxed or non-existent intellectual property restrictions. For Open Source Security this allows users to create user-generated software content and advice through incremental individual effort or through collaboration.

Pharming: Pharming is a hackers attack aiming to redirect a website's traffic to another website, like cattle rustlers herding the bovines in the wrong direction. The destination website is usually bogus.

Phishing: Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Phishing is typically carried out using e-mail (where the communication appears to come from a trusted website) or an instant message, although phone contact has been used as well.

Registrars: A domain name registrar is a company with the authority to register domain names, authorized by ICANN.

Rogue Software: Rogue security software is software that uses malware (malicious software) or malicious tools to advertise or install its self or to force computer users to pay for removal of nonexistent spyware. Rogue software will often install a trojan horse to download a trial version, or it will execute other unwanted actions.

Rootkit: A set of software tools used by a third party after gaining access to a computer system in order to conceal the altering of files, or processes being executed by the third party without the user's knowledge.

Sandnet: A sandnet is closed environment on a physical machine in which malware can be monitored and studied. It emulates the internet in a way which the malware cannot tell it is being monitored. Wonderful for analyzing the way a bit of malware works. A Honeynet is the same sort of concept but more aimed at attackers themselves, monitoring the methods and motives of the attackers.

Spam: Spam is the term widely used for unsolicited e-mail. . Spam is junk mail on a mass scale and is usually sent indiscriminately to hundreds or even hundreds of thousands of inbox's simultaneously.

Trojans: Also known as a Trojan horse, this is Software that appears to perform or actually performs a desired task for a user while performing a harmful task without the user's knowledge or consent.

Worms: A malicious software program that can reproduce itself and spread from one computer to another over a network. The difference between a worm and a computer virus is that a computer virus attaches itself to a computer program to spread, while a worm is self-contained and can send copies of itself across a network.

Appendix 3: Atrivo – Abuse CastleCops Log

Information relating to Atrivo not responding to abuse complaints – Ref CastleCops.

CastleCops' Spam Incident Reporting and Termination and Malware Incident Reporting and Termination volunteers log malware and porn spam incidents and make abuse complaints. Below are 4 typical examples of Atrivo not responding to these complaints, where we have turnover in Atrivo domains, it is an attempt to evade blacklists.

CASE 1:

Query result: 7-7-2008

<http://www.robtext.com/dns/spycrush.com.html>
spycrush.com

information about spycrush.com is fresh

spycrush.com is a domain controlled by three nameservers at spycrush.biz. All of them are on different IP networks. Incoming mail for spycrush.com is handled by one mailserver at spycrush.com themselves. spycrush.com has one IP record .

base record name ip reverse route as

spycrush.com a 85.255.117.206 85.255.116.0/23 Atrivo AS27595

ATRIVO AS Atrivo

Complaint Dates: 8-11-2007 and 1-15-2008

http://www.castlecops.com/FraudTool_malware757.html

status: confirmed malware

HTTP Response

07 Jul, 2008

22:16:46 HTTP/1.1 302 Found

HTTP/1.1 302 Found

HTTP/1.1 200 OK

ID 757 (termination link)

Title FraudTool

Entry <http://www.spycrush.com/download.php>

MIRT Squad

Reporter trshaw

Timestamp 11 Aug, 2007 @ 20:47:35

Topic ID 212878 - Read/respond to MIRT commentary.

Handler Note:

15 Jan, 2008

02:22:45 tactick: sc_setup.exe at this location is malware known as FraudTool.Win32.SpyHeal.f (Kaspersky)

Handler Note:

15 Jan, 2008

02:47:15 tactick: View CIDR AS27595 Report:

<http://www.cidr-report.org/cgi-bin/as-report?as=27595>

"27595 | US | arin | 2003-04-07 | INTERCAGE - InterCage, Inc."

Handler Note:

15 Jan, 2008

02:47:16 tactick: Extended information for AS27595:

State/Province: ca

Country: us

Responsible Domain: atrivo.com

Abuse Email: abuse@atrivo.com

Handler Note:

15 Jan, 2008

03:07:25 tactick: Generated and sent email malware alert to respective parties.

Fetchd URLs <http://www.spycrush.com/download.php>

CASE 2:

Query result: 7-7-2008

<http://www.robtext.com/dns/codecmega.com.html>

base	record	name	ip	reverse	route	as
codecmega.com	a		64.28.184.188		64-28-184-188-rev.cernel.net	
		64.28.176.0/20	Atrivo	AS27595	ATRIVO AS	Atrivo
ns	ns1.popcodec.net		64.28.184.164		64-28-184-164-rev.cernel.net	
	ns2.popcodec.net		64.28.184.165		64-28-184-165-rev.cernel.net	
	ns1.codecmega.com		64.28.181.226		64-28-181-226-rev.cernel.net	
	ns2.codecmega.com		64.28.181.227		64-28-181-227-rev.cernel.net	
mx	mail.codecmega.com		64.28.181.226		64-28-181-226-rev.cernel.net	

Complaint Date: 5-13-2008

http://www.castlecops.com/Trojan_Dropper_malware11439.html

status: confirmed malware

HTTP Response

07 Jul, 2008

03:15:59 408 - SIRT Operation Timed Out
ID 11439 (termination link)
Title Trojan-Dropper
Entry <http://codecmega.com/download/codecmega4035.exe>
MIRT Squad
Reporter DarthTrader
Timestamp 11 May, 2008 @ 17:22:41
Topic ID 221707 - Read/respond to MIRT commentary.
Handler Note:
13 May, 2008
00:27:22 tetak: codecmega4035.exe at this location is malware known as
TrojanDropper:Win32/Alureon.C (Microsoft).
Handler Note:
13 May, 2008
00:29:41 tetak: View CIDR AS27595 Report:
<http://www.cidr-report.org/cgi-bin/as-report?as=27595>

"27595 | US | arin | 2003-04-07 | INTERCAGE - InterCage, Inc."

Handler Note:
13 May, 2008
00:29:41 tetak: Extended information for AS27595:
State/Province: ca
Country: us
Responsible Domain: atrivo.com
Abuse Email: abuse@atrivo.com
Handler Note:
13 May, 2008
00:29:58 tetak: Generated and sent email malware alert to respective parties.

CASE 3:

Query result: 7-7-2008
<http://www.robtx.com/dns/5yearscontract.com.html>
base record name ip reverse route as
5yearscontract.com a 58.65.239.114 58-65-239-114.myrdns.com
58.65.239.0/24 Atrivo AS27595 ATRIVO AS Atrivo
ns ns1.ipnames.net 202.75.33.138 202.75.32.0/22 Proxy-registered
route object AS17464 TMIDC AP Hosting Services (MYLOCA), Data
Services Division, Telekom Malaysia
ns2.ipnames.net 124.217.240.5 124.217.240.0/20 Proxy-registered
route object AS9930 TTNET MY TIMEDOTCOM BERHAD

mx mail.5yearscontract.com 58.65.239.114 58-65-239-114.myrdns.com
58.65.239.0/24 Atrivo AS27595 ATRIVO AS Atrivo

Complaint Date: 2-1-2008

http://www.castlecops.com/Trojan_Downloader_malware7724.html

status: confirmed malware

HTTP Response

07 Jul, 2008

03:07:51 HTTP/1.1 200 OK

ID 7724 (termination link)

Title Trojan-Downloader

Entry <http://5yearscontract.com/check/n14041.htm>

MIRT Squad

Reporter tetak

Timestamp 01 Feb, 2008 @ 03:25:09

Topic ID 214588 - Read/respond to MIRT commentary.

Handler Note:

01 Feb, 2008

23:35:46 tetak: n14041.htm at this location is malware called
Trojan-Downloader.JS.Agent.bdy (Kaspersky)

Handler Note:

01 Feb, 2008

23:36:11 tetak: View CIDR AS27595 Report:

<http://www.cidr-report.org/cgi-bin/as-report?as=27595>

"27595 | US | arin | 2003-04-07 | INTERCAGE - InterCage, Inc."

Handler Note:

01 Feb, 2008

23:36:12 tetak: Extended information for AS27595:

State/Province: ca

Country: us

Responsible Domain: atrivo.com

Abuse Email: abuse@atrivo.com

Handler Note:

01 Feb, 2008

23:39:39 tetak: Generated and sent email malware alert to respective parties.

CASE 4:

Query result: 7-7-2008

<http://www.robtext.com/dns/spylocked.com.html>

spylocked.com

information about spylocked.com is fresh

spylocked.com is a domain controlled by three nameservers at wildgadgets.biz. All of them are on different IP networks. Incoming mail for spylocked.com is handled by one mailserver at spylocked.com themselves. spylocked.com has one IP record .

base record name ip reverse route as

spylocked.com a 85.255.120.50 85.255.120.0/24 Atrivo AS27595

ATRIVO AS Atrivo

ns ns1.wildgadgets.biz 195.3.144.77 antispysupport.com
195.3.144.0/22 Cronos IT Network AS41390 CRONOSIT AS CronosIT

Autonomous System

ns2.wildgadgets.biz 81.95.145.186 ?

ns3.wildgadgets.biz 85.255.114.202 85.255.114.0/23 Atrivo AS27595

ATRIVO AS Atrivo

Complaint Date: 1-15-2008

http://www.castlecops.com/FraudTool_malware756.html

status: confirmed malware

HTTP Response

07 Jul, 2008

22:16:33 HTTP/1.1 302 Found

HTTP/1.1 302 Found

HTTP/1.1 200 OK

ID 756 (termination link)

Title FraudTool

Entry http://spylocked.com/download_final.php

MIRT Squad

Reporter trshaw

Timestamp 11 Aug, 2007 @ 20:47:07

Topic ID 212881 - Read/respond to MIRT commentary.

Handler Note:

15 Jan, 2008

03:16:12 tacttick: sl_setup.exe at this location is malware known as

FraudTool.Win32.MalwareWipe.q (Kaspersky)

Handler Note:

15 Jan, 2008

03:23:07 tacktick: View CIDR AS27595 Report:

<http://www.cidr-report.org/cgi-bin/as-report?as=27595>

"27595 | US | arin | 2003-04-07 | INTERCAGE - InterCage, Inc."

Handler Note:

15 Jan, 2008

03:23:08 tacktick: Extended information for AS27595:

State/Province: ca

Country: us

Responsible Domain: atrivo.com

Abuse Email: abuse@atrivo.com

Handler Note:

15 Jan, 2008

03:24:51 tacktick: Generated and sent email malware alert to respective parties.

Fetches URLs http://spylocked.com/download_final.php