The Twisted Family Tree of the Transponder Gang

Joe Telafici & Seth Purdy
McAfee® AVERT™
October 7, 2005

What's in a name?

- Netbus 2.0 was our first non-malicious detection (Application type); 1.0 was a Trojan.
- Only significant difference was that it was sold and marketed as a remote control app.
- Difference between Trojan and Spyware may be as little as the presence of a EULA.
- This may require an expanded analysis, not only of the software in question, but the entity that produces it, and the context in which it is deployed.
- **Are our tools and procedures up to this task?**

Why Direct Revenue?

- A new researcher stumbled across a number of similarities in several apparently distinct pieces of adware
- WebHelper's Transponder Gang site[1] seemed to link many different companies together
- Other Anti-Spyware and AntiVirus companies seemed to differ, sometimes radically, in naming
- Using naïve techniques available to normal malware researchers, would we be able to prove or disprove connections, or would we need to develop new tools and processes?

[1] http://www.webhelper4u.com/

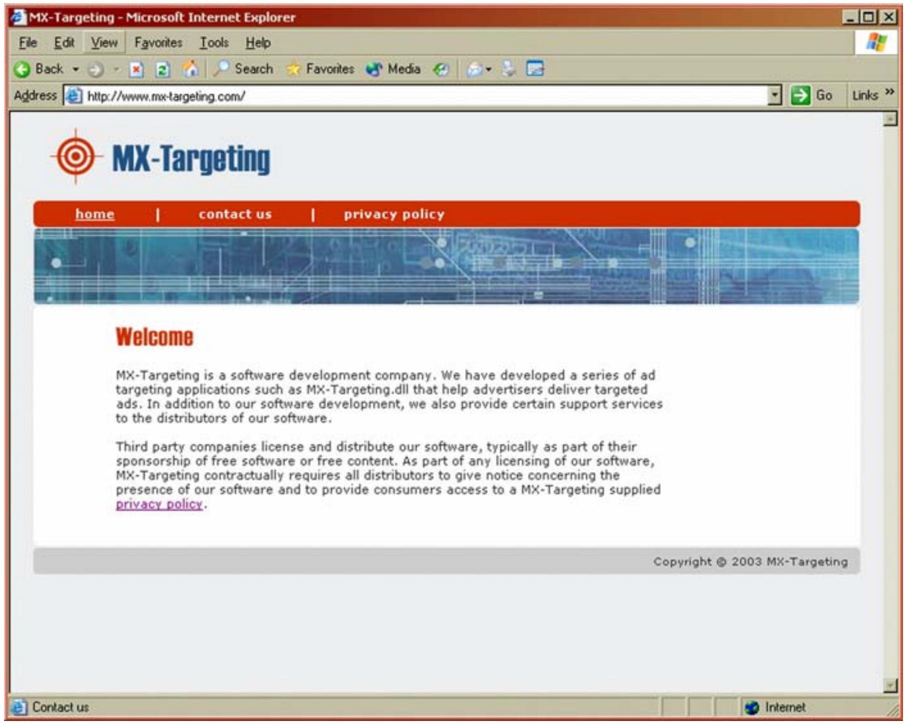
The problem statements

- Using only readily-available tools and public data sources, what can we discover about the companies that make Adware or Spyware?
- What can we learn about the business model using these techniques?
- Can we learn enough to correctly identify related threats in this space?
- Could our customers achieve enough of an understanding of the vendor to form a meaningful trust relationship?

Easily observed - the initial data

- Multiple individual samples with separate branding and company web presences
  - www.pynix.com
  - www.mx-targeting.com
  - www.twain-tech.com
  - Others are similar with slight differences (btgrab.com, others)

Nearly identical website structure and text templates

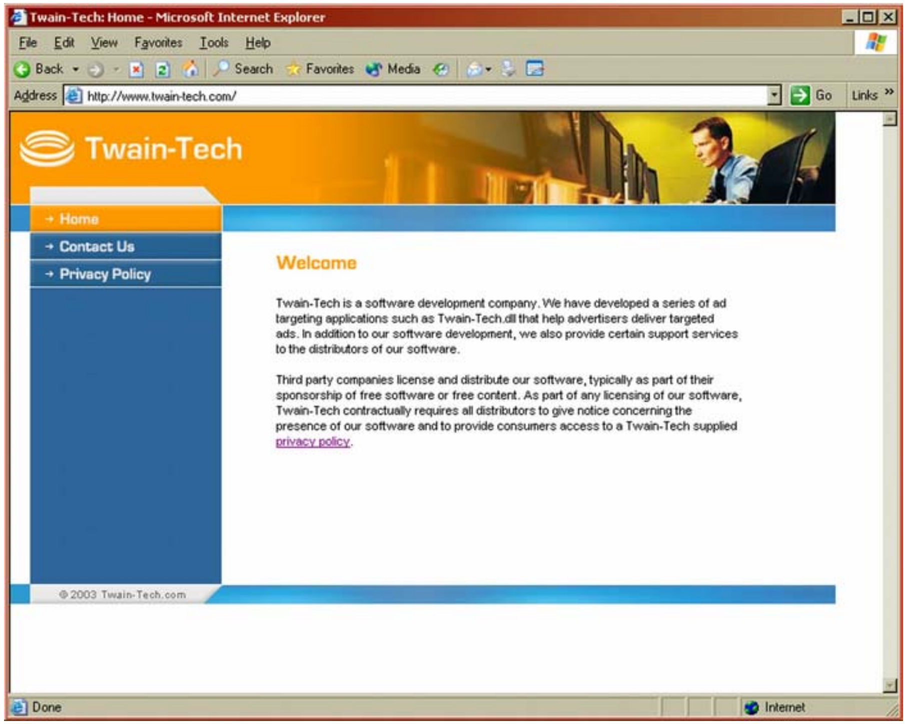

MX-Targeting - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.mx-targeting.com/
Go Links »
MX-Targeting
home | contact us | privacy policy
Contact us
Internet

Welcome

MX-Targeting is a software development company. We have developed a series of ad targeting applications such as MX-Targeting.dll that help advertisers deliver targeted ads. In addition to our software development, we also provide certain support services to the distributors of our software.

Third party companies license and distribute our software, typically as part of their sponsorship of free software or free content. As part of any licensing of our software, MX-Targeting contractually requires all distributors to give notice concerning the presence of our software and to provide consumers access to a MX-Targeting supplied privacy policy.

Copyright © 2003 MX-Targeting


Twain-Tech: Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.twain-tech.com/
Go Links »
Twain-Tech
→ Home
→ Contact Us
→ Privacy Policy
Done
Internet

Welcome

Twain-Tech is a software development company. We have developed a series of ad targeting applications such as Twain-Tech.dll that help advertisers deliver targeted ads. In addition to our software development, we also provide certain support services to the distributors of our software.

Third party companies license and distribute our software, typically as part of their sponsorship of free software or free content. As part of any licensing of our software, Twain-Tech contractually requires all distributors to give notice concerning the presence of our software and to provide consumers access to a Twain-Tech supplied privacy policy.

© 2003 Twain-Tech.com

Server-driven run-time behavior

- Similarities in functionality (tracking browsing behavior)
- Same high-level protocol utilized
- Self-update occurring from one product to another
- Common host destinations for network communication

Similarities in Functionality

- ▶ All utilize Browser Helper Object DLLs
- ▶ Interception and transmission of URLs and keywords during browsing
- ▶ Retrieval of advertisements as directed by a controller server (presumably based on transmitted data)
- ▶ Similar initial configuration and update procedure

Common High-Level Protocol

- Twaintec.dll

GET /twain/servlet/Twain?**adcontext=ROUTINE_CHECKIN**&contextpeak=0&contextcount=0&countrycodein=XX&lastAdTime=0&lastAdCode=0&cookie1=0&cookie2=0&cookie3=0&cookie4=0&**InstID**={09C19EB0-6F3A-4252-A422-DD2493EF2366}&status=1&smode=1&**bho=twaintec.dll**&NumWindows=2&PartnerId=0&BundleId=0&HN=Easystreet-spurdy-vm&VSN=58F7EC7C&PI=55274-337-4451957-22511&MA=000C2943A358 HTTP/1.1

User-Agent: {09C19EB0-6F3A-4252-A422-DD2493EF2366}|0.1.4.67

Host: **ctl.twain-tech.com**

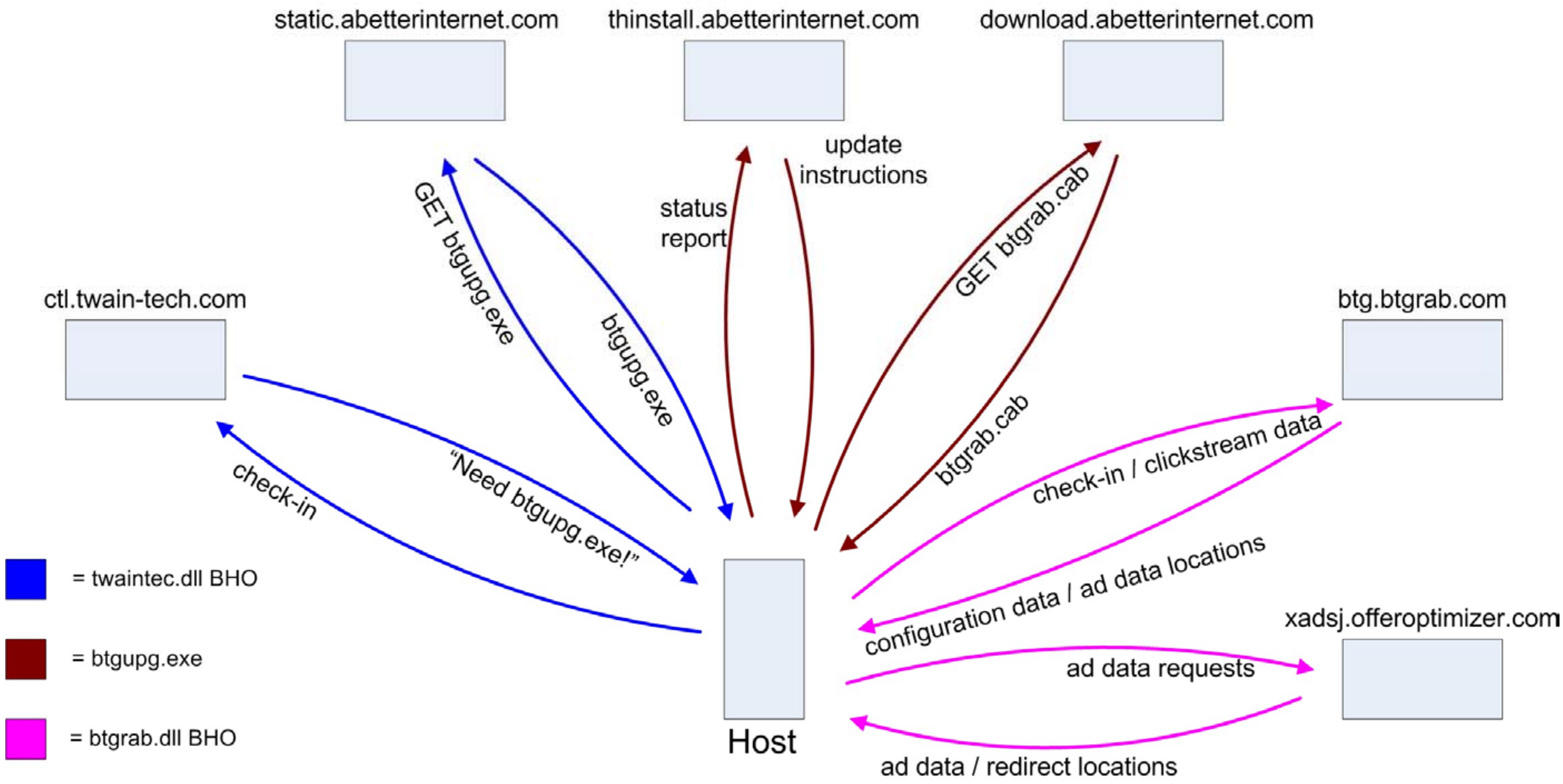
- Btgrab.dll

GET /a/Drk.syn?**adcontext=ROUTINE_CHECKIN**&contextpeak=0&contextcount=0&countrycodein=XX&lastAdTime=0&lastAdCode=0&cookie1=0&cookie2=0&cookie3=0&cookie4=0&**InstID**={AC9E78A0-5F78-4BB7-BBFE-13801C8AD531}&DistID=NA&status=1&smode=1&**bho=BTGrab.dll**&NumWindows=2&PartnerId=0&BundleId=0&HN=Easystreet-spurdy-vm&VSN=58F7EC7C&PI=55274-337-4451957-22511&MA=000C2943A358 HTTP/1.1

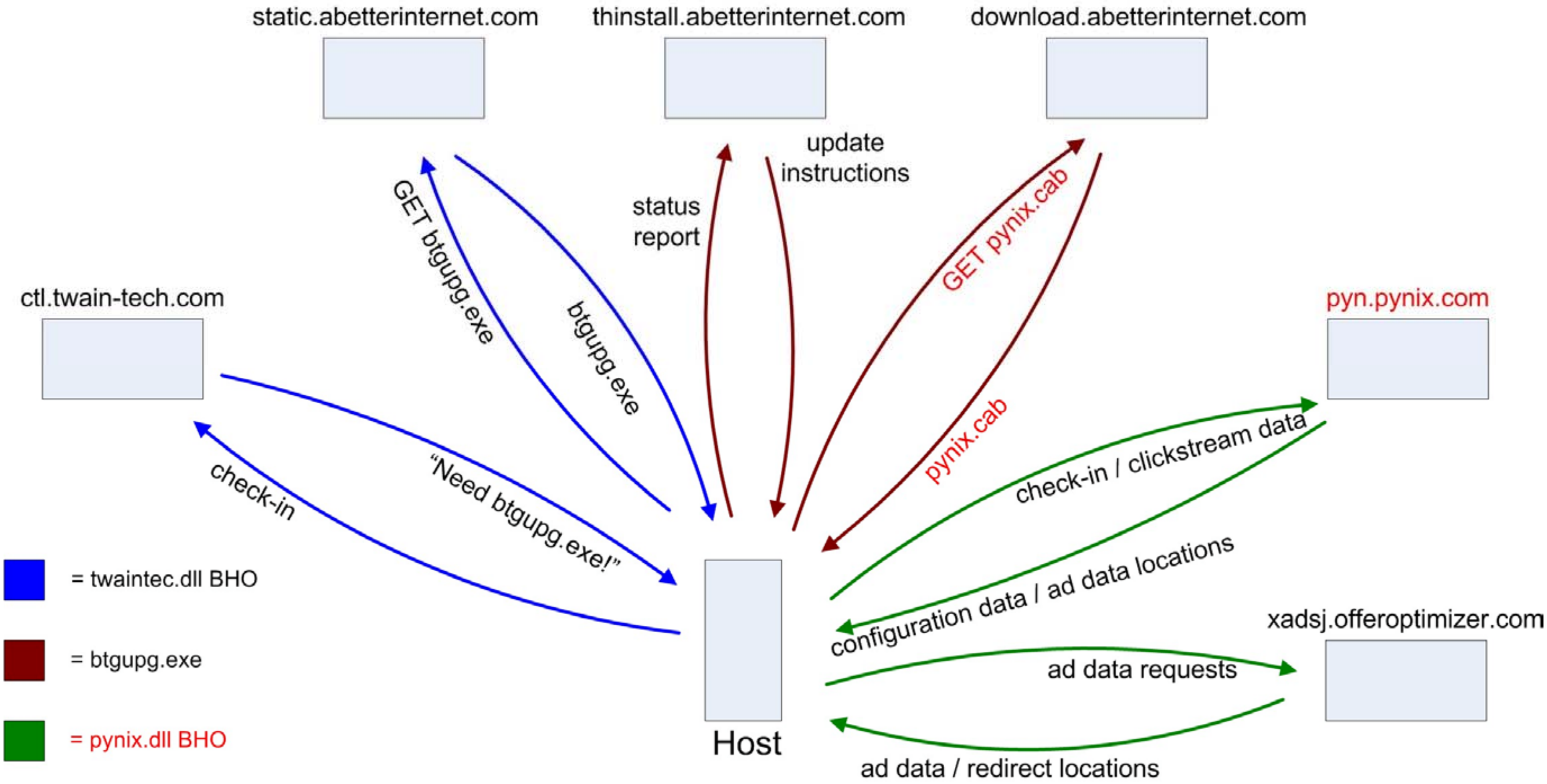
User-Agent: {AC9E78A0-5F78-4BB7-BBFE-13801C8AD531}|0.9.4.67

Host: **btg.btgrab.com**

Self-Update Between Products
(2/11/05, twaintec.dll to btgrab.dll)



Self-Update Between Products
(5/13/05, twaintec.dll to pynix.dll)



🟦 = twaintec.dll BHO

🟥 = btgupg.exe

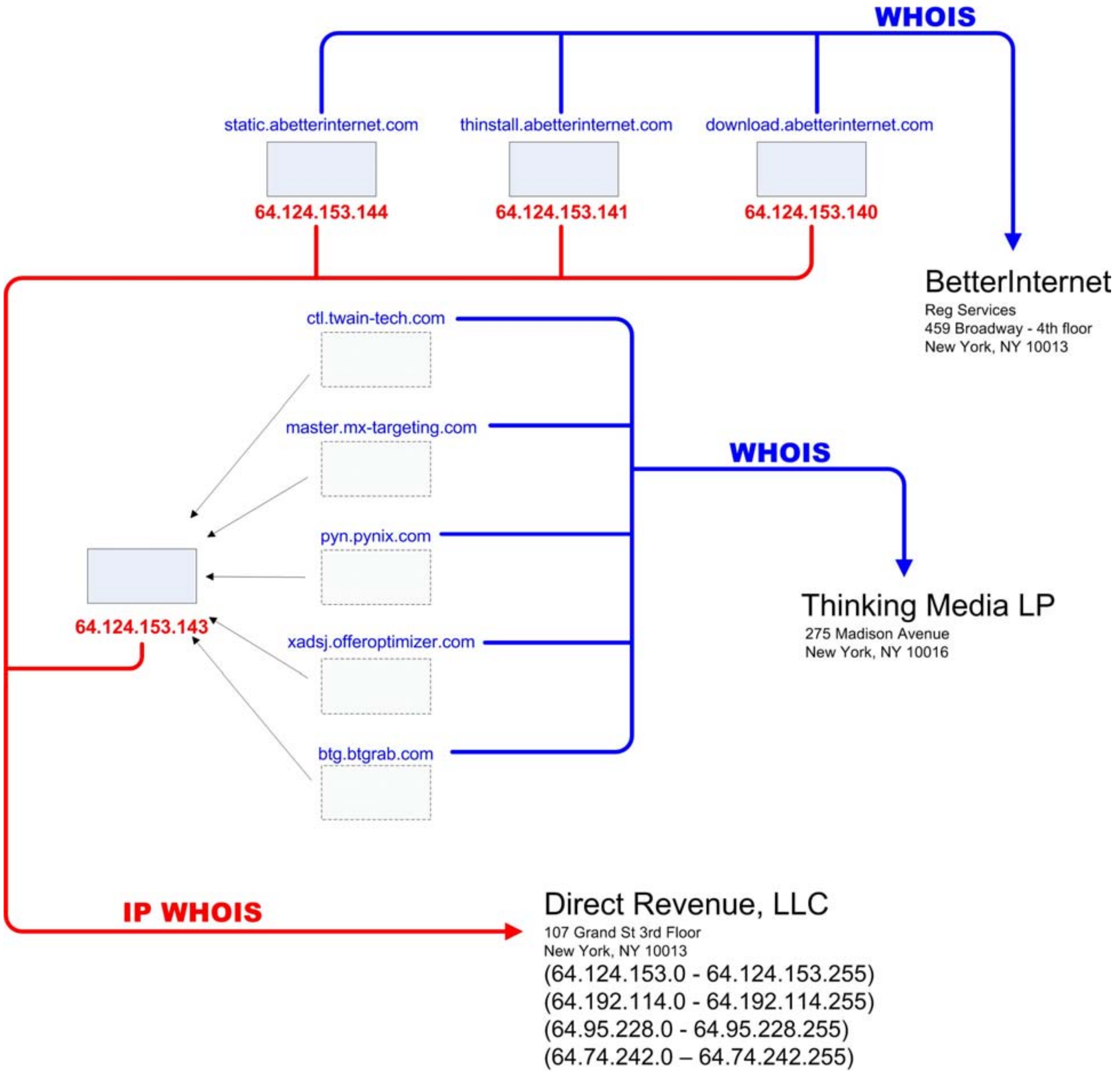
🟩 = pynix.dll BHO

Common Host Destinations

- ▶ twaintec.dll
  - ctl.twaintec.com – 64.174.242.143
  - static.abetterinternet.com, xadsj.offeroptimizer.com
- ▶ pynix.dll
  - pyn.pynix.com - 64.174.242.143
  - static.abetterinternet.com, xadsj.offeroptimizer.com
- ▶ mxtarget.dll
  - master.mx-targeting.com – 64.174.242.143
  - static.abetterinternet.com, xadsj.offeroptimizer.com

Untangling the Net

- ▶ Correlation of destination addresses
  - Multiple overlaps in domain and IP ranges of contacted hosts across the samples
  - Use of IP address rotation among several Class C ranges for the servers and domains contacted
  - Setup is a four-way round-robin amongst hosts on four different networks with 30 second TTLs
- ▶ Reverse DNS and WHOIS records
  - Reveal common registrants spanning these destinations



WHOIS

static.abetterinternet.com

64.124.153.144

thinstall.abetterinternet.com

64.124.153.141

download.abetterinternet.com

64.124.153.140

BetterInternet
Reg Services
459 Broadway - 4th floor
New York, NY 10013

ctl.twain-tech.com

master.mx-targeting.com

pyn.pynix.com

xadsj.offeroptimizer.com

btg.btgrab.com

64.124.153.143

WHOIS

Thinking Media LP
275 Madison Avenue
New York, NY 10016

IP WHOIS

Direct Revenue, LLC
107 Grand St 3rd Floor
New York, NY 10013
(64.124.153.0 - 64.124.153.255)
(64.192.114.0 - 64.192.114.255)
(64.95.228.0 - 64.95.228.255)
(64.74.242.0 – 64.74.242.255)

From Bits to Boardrooms

- Armed with several implications from technical analysis we begin to look at the surrounding business organizations
  - Research state records of incorporation
  - Examine ownership of relevant domains and IPs
  - View archived web sites to fill in the blanks
- Why is this relevant?
  - Naming
  - Generic or heuristic detection
  - Trojan vs. PUP designations
  - Version info is unreliable

Assembling the Big Picture - Domains

- Public web pages are co-located at hosting sites like Readyhosting (TX) and rackspace.com, but download and config servers hosted directly by DR.
- Domain names contacted by likely DR software are largely registered to a company called Thinking Media, LP.
- We could not locate any relevant data about this company
- However historical whois info shows some links:
  - Offeroptimizer.com originally registered to an A. Murray
  - VX2.org originally registered to a Joshua Abram
  - IPinsight.com originally registered to a Daniel Kaufman
  - All three names listed as officers for one or more of TrueData Corporation, IPInsight, Direct Revenue, CPV Market, Dash.com

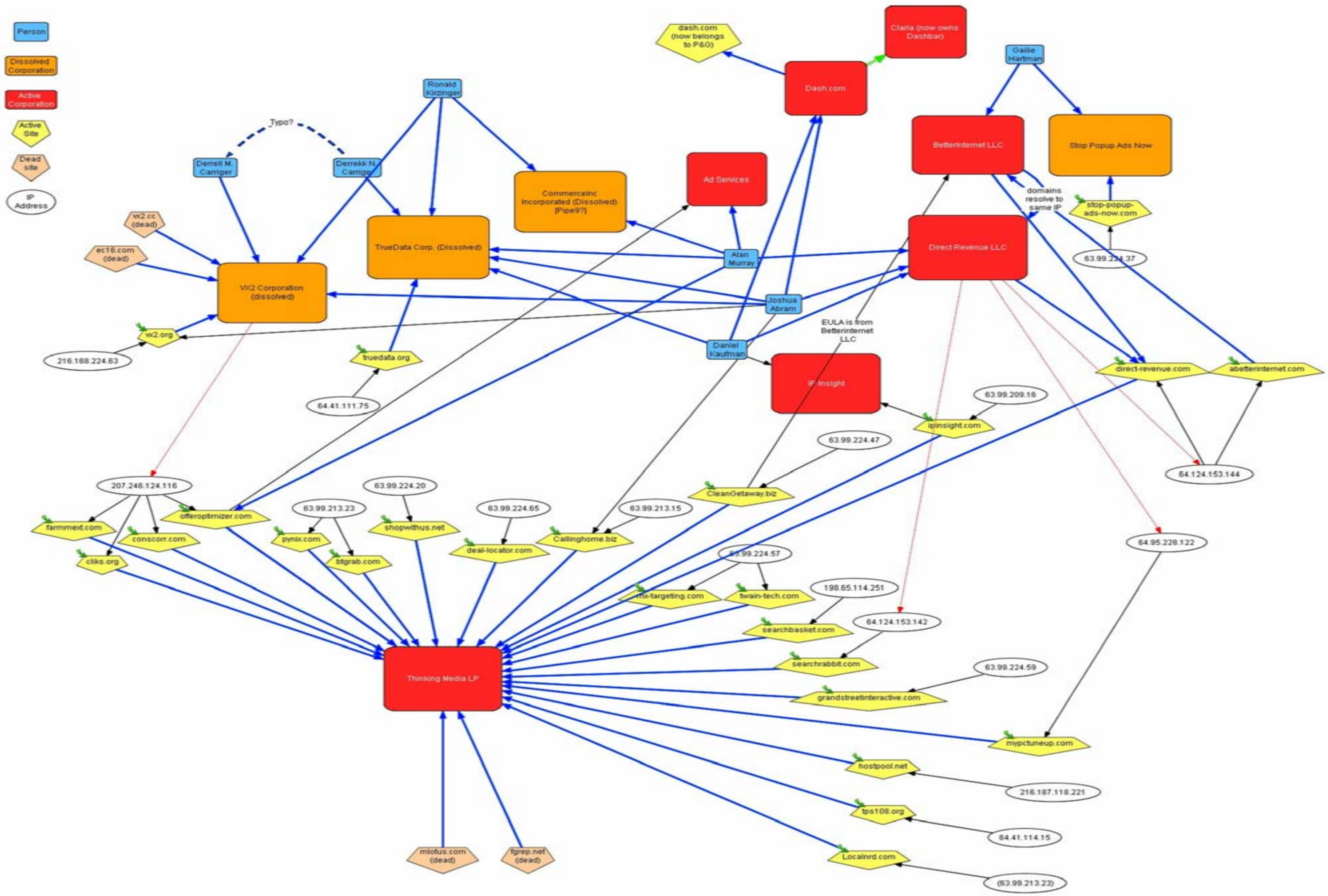
Assembling the Big Picture - Incorporation

- Incorporation records:
  - In the US, incorporation varies state-to-state
  - Public databases available in about 29 of 50 states
  - Information available varies widely
  - Some require a fee

Assembling the Big Picture - Incorporation

- Most DR-related companies based in New York, but incorporated in Nevada
- Nevada lists officers that differ from those listed on the web sites, and are likely phony, or represent the registering agent, e.g. Derrell M. Carriger, Derrekk N. Carriger, Gailie Hartman also listed for hundreds of other companies.
- Addresses for companies match those of the registering agent, not the company itself.
- Though most companies we could find have dissolved, matching domain names up and registered to Thinking Media or resolve to DR IP range

The Transponder Family



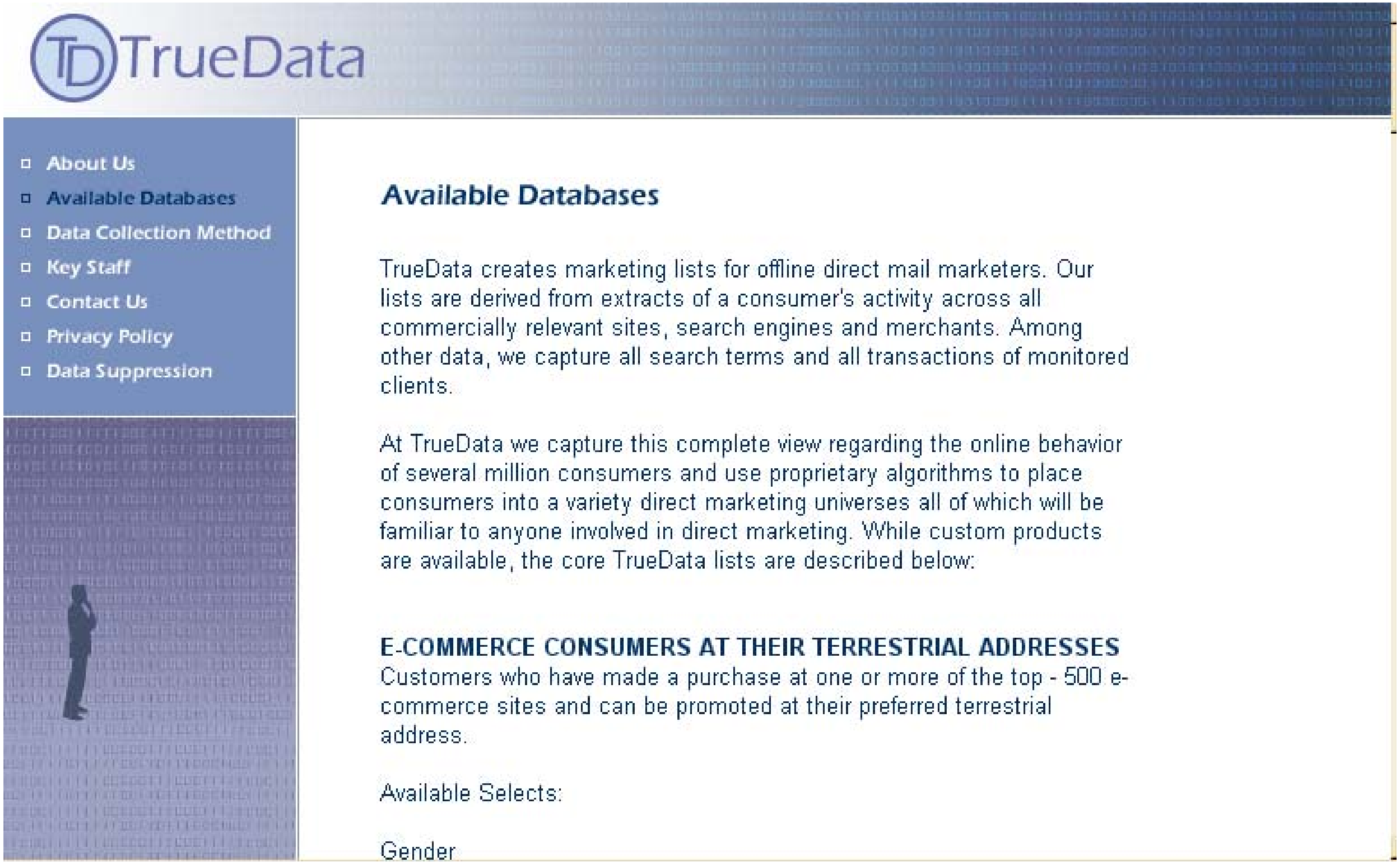
Archival web data

- Archive.web.org maintains some historical data for publicly-available pages
- Fortunately, the web sites of DR-related companies frequently listed the officers of said companies: Direct Revenue, Truedata.org, IPInsight all list one or more of
  - Daniel Kaufman
  - Joshua Abram
  - Alan Murray
  - Rodney Hook
- Names correlate with some of those in domain registrations, incorporation records

Archival web data - continued

- Perhaps more interesting are some of the claims made by former companies to potential advertisers
  - Can link very specific online transactions with particular web sites to consumers terrestrial addresses (truedata.org)
  - Some things tracked include:
    - Details about computer and ISP
    - Hours spent at banking or brokerage sites
    - Gender of consumers
    - Job-seeking
    - Car shopping at particular sites
  - Can locate consumers with over 600 demographic variables based solely on IP address (ipinsight.com)

Yikes!



Available Databases

TrueData creates marketing lists for offline direct mail marketers. Our lists are derived from extracts of a consumer's activity across all commercially relevant sites, search engines and merchants. Among other data, we capture all search terms and all transactions of monitored clients.

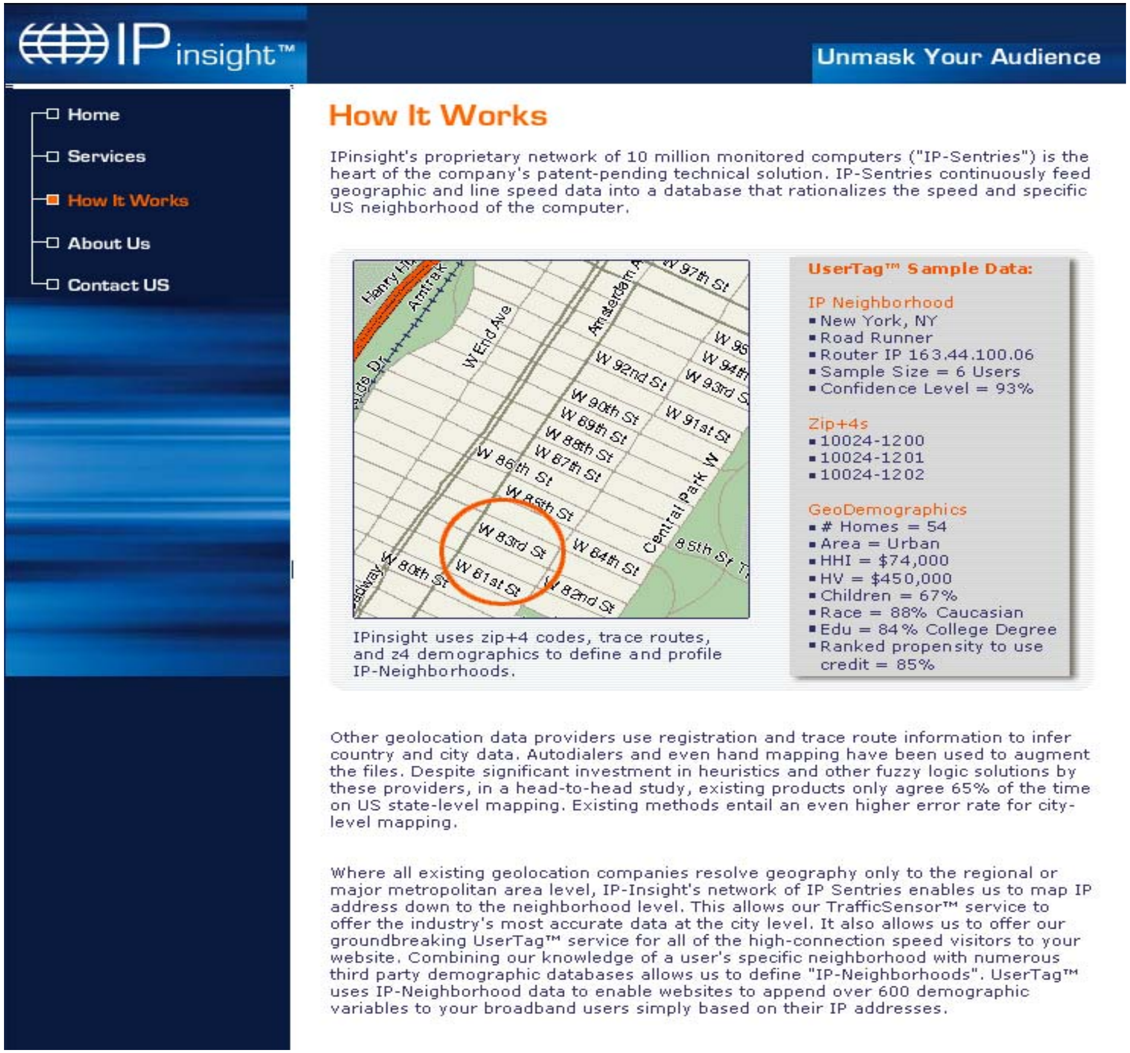
At TrueData we capture this complete view regarding the online behavior of several million consumers and use proprietary algorithms to place consumers into a variety direct marketing universes all of which will be familiar to anyone involved in direct marketing. While custom products are available, the core TrueData lists are described below:

E-COMMERCE CONSUMERS AT THEIR TERRESTRIAL ADDRESSES
Customers who have made a purchase at one or more of the top - 500 e-commerce sites and can be promoted at their preferred terrestrial address.

Available Selects:

Gender

Eeeek!



How It Works

IPinsight's proprietary network of 10 million monitored computers ("IP-Sentries") is the heart of the company's patent-pending technical solution. IP-Sentries continuously feed geographic and line speed data into a database that rationalizes the speed and specific US neighborhood of the computer.

IPinsight uses zip+4 codes, trace routes, and z4 demographics to define and profile IP-Neighborhoods.

UserTag™ Sample Data:

IP Neighborhood
- New York, NY
- Road Runner
- Router IP 163.44.100.06
- Sample Size = 6 Users
- Confidence Level = 93%

Zip+4s
- 10024-1200
- 10024-1201
- 10024-1202

GeoDemographics
- # Homes = 54
- Area = Urban
- HHI = $74,000
- HV = $450,000
- Children = 67%
- Race = 88% Caucasian
- Edu = 84% College Degree
- Ranked propensity to use credit = 85%

Other geolocation data providers use registration and trace route information to infer country and city data. Autodialers and even hand mapping have been used to augment the files. Despite significant investment in heuristics and other fuzzy logic solutions by these providers, in a head-to-head study, existing products only agree 65% of the time on US state-level mapping. Existing methods entail an even higher error rate for city-level mapping.

Where all existing geolocation companies resolve geography only to the regional or major metropolitan area level, IP-Insight's network of IP Sentries enables us to map IP address down to the neighborhood level. This allows our TrafficSensor™ service to offer the industry's most accurate data at the city level. It also allows us to offer our groundbreaking UserTag™ service for all of the high-connection speed visitors to your website. Combining our knowledge of a user's specific neighborhood with numerous third party demographic databases allows us to define "IP-Neighborhoods". UserTag™ uses IP-Neighborhood data to enable websites to append over 600 demographic variables to your broadband users simply based on their IP addresses.

Recent activities

- Mypctuneup.com site set up to uninstall many likely VX2-based pieces of software, but makes no implication of ownership, responsibility or relationship to Direct Revenue or ABetterInternet
- Formerly in-the-clear transmissions are now encrypted
- Different locations for public web sites and backend servers makes some correlation possible to the dedicated researcher, but further obscures apparent public relationships

What can we say about Direct Revenue?

▶ Surprisingly little, conclusively

- Same people seem to be involved in a wide variety of companies with similar business models and practices over the years
- Most web sites (Twain-tech, MX-Targeting, Farmmext.com) seem to be shells only with no apparent corporate relationship
- Interrelationships of companies, people, sites and software are present, but tenuous
- It is unclear whether the lack of transparency is deliberate or an artifact, but definitely present
- The degree of personal information tracking and correlation seems huge, at least in past entities
- Recent activities seem mixed in terms of commitment to transparency

What can we say about our research tools and methods?

- Even for large U.S. corporations, relevant information is scarce, hard-to-find or absent
- Existing archives of domain registration, DNS history and incorporation data do not allow for the kind of queries that would allow for a complete picture
  - Incorporation records vary too widely, often unavailable
  - No way to know which state a corporation is registered in
  - No way to locate all domains registered to a particular company
  - Existing privacy mechanisms (anonymous hosting and domain name services, opt-out of archiving) may hamper investigation further
- Situation in other parts of the world likely more grim

The implications

- Static and dynamic analysis is still one of the most useful tools for relating software
  - Coding similarities
  - Unique strings
  - Commonality of IP addresses contacted, communication protocols
- Cooperation with law enforcement or other dedicated investigators will be required to make any definitive assertions
- Industry-level cooperation on DNS information, particularly, and other areas would help considerably
- The effort required to arrive at even this level of detail is prohibitive (several man-weeks)

Questions