Using Traffic Direction Systems to simplify fraud... and complicate investigations!

Maxim Goncharov
What is web traffic?

User ——> Site
Separate Web traffic?

User → Script-in-the-middle → Site

User → Site

User → Site

User → Site
System to separate traffic?

User → Script-in-the-middle → Site

- Database
- Control Panel
- Statistics
- Filtering

TDS Traffic Direction System
VB2011 - the 21st Virus Bulletin International
Traffic Direction System?
Fingerprint

GET /1/1/typical.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, application/x-shockwave-flash, */*
Referer: http://www.trendmicro.com/news
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)
Host: www.just-a-stie.com
Connection: Keep-Alive

browser
language
OS
referer
Main TDS functionality

Traffic Direction System
Main TDS functionality

Traffic Direction System

Control traffic directions

By Browser

By OS

By Geo location

By Time

By Referrer
Main TDS functionality

Traffic Direction System

Control traffic directions
- By Browser
- By OS
- By Geo location
- By Time
- By Referrer

Filter non wished traffic
- By Know IP Subnets
- By Search Engine Ref.
- By already seen IPs
Main TDS functionality

Traffic Direction System

Control traffic directions
- By Browser
- By OS
- By Geo location
- By Time
- By Referrer

Filter non wished traffic
- By Know IP Subnets
- By Search Engine Ref.
- By already seen IPs

Collect statistics
- For Partnerka
- For Referrals
- Into Database
Areas of usage.

Traffic Direction System

Farma  Black SEO  Exploit  Adult  SMS
Volume makes money

Traffic Direction System

More visitors = more profits!
Web User Fraud: `<iframe>`
Web User Fraud: `<iframe/>`
Web User Fraud: `<iframe/>`

TDS Traffic Direction System

EN

DE

FR

ES
Web User Fraud: `<iframe/>`

Traffic Direction System

TDS Traffic Direction System

VB2011 - the 21st Virus Bulletin International
Web User Fraud: `<iframe>`

**TDS Traffic Direction System**

- **DE** + **XP** + **IE**
- **DE** + **95** + **IE**
- **DE** + **XP** + **MZ**
- **DE** + **V** + **IE**
- **DE** + **7** + **IE**

---

**max_goncharov@trendmicro.com** @ppats77

**Tuesday, October 18, 11**

**TDS Traffic Direction System**

VB2011 - the 21st Virus Bulletin International
Malware Vector TDS

Traffic Direction System

MPack
Phenix
Eleonore
Malware Vector multi layer TDS

Eleonore

MPack

Phenix

Traffic Direction System #1

Traffic Direction System #2

Traffic Direction System #3

iframe

max_goncharov@trendmicro.com

e@ppats77
Partnerka is an affiliate marketing program, in which the partners are payed off for online distribution of legal or illegal content.
TDS Partnerka - Possible fraud

TDS Partnerka is an affiliate marketing program, in which the partners are payed off for exchange of the Web Traffic and its monetization.
TDS Partnerka - Possible fraud

max_goncharov@trendmicro.com
@ppats77

Tuesday, October 18, 11
TDS Software

Web Server

Application

Database

Apache

NGINX

php

MySQL

CGI

PostgreSQL
TDS Software

Simple TDS
Sutra TDS
Crazy TDS
Kalisto TDS
ILTDS
Advanced TDS
Keitaro TDS
TDS Software

- Simple TDS
- Sutra TDS
- Crazy TDS
- Kalisto TDS
- ILTDS
- Advanced TDS
- Keitaro TDS
Traffic Fraud using TDS

intentional

traffic sold to PPI

unintentional

traffic sold to the traffic market

traffic paid as usage fee of the TDS software

traffic paid as usage fee of the TDS service

stolen traffic
Traffic Fraud using TDS

traffic sold to the traffic market

User HTTP Request → Web Site IFrame → TDS sends to Traffic Market → HTTP request bought by PPI → HTTP Exploit attack the User
Traffic Fraud using TDS

- User HTTP Request
- Web Site IFrame
- TDS sends traffic to the hidden gateway
- Hidden gateway sale the traffic
- HTTP Exploit attack the User

stolen traffic
TDS for ransomware
Ransomware example

crawler
US IP Address
+ en-gb header

TDS Direct traffic by Geo IP and Language

French IPs

Binary drop page

Mixed IPs

Re-Sale traffic TDS

TDS Traffic Direction System

max_goncharov@trendmicro.com
@ppats77

TDS2011 - the 21st Virus Bulletin International
Ransomware example

crawler
RU IP Address +
ru header

TDS Direct traffic by Geo IP and Language

French IPs

Binary drop page

Mixed IPs

Re-Sale traffic TDS

TDS Traffic Direction System

max_goncharov@trendmicro.com
e@ppats77

TDS Traffic Direction System

VB2011 - the 21st Virus Bulletin International
Detecting TDS

Analytic

Synthetic

request

result
Detecting TDS

Analytic

TDS Traffic Direction System

max_goncharov@trendmicro.com
@ppats77

Tuesday, October 18, 11
Detecting TDS

IP

Analytic

85.114.156.56
Detecting TDS

Analytic

IP

EN-US / DE / FR / RU

Language

85.114.156.56
Detecting TDS

- IP: 85.114.156.56
- Language: EN-US / DE / FR / RU
- Browser: Mozilla / IE / Safari

TDS Traffic Direction System

VB2011 - the 21st Virus Bulletin International
Detecting TDS

IP: 85.114.156.56
Language: EN-US / DE / FR / RU
Browser: Mozilla / IE / Safari
OS: Win95 / WinXP / MacOS

TDS Traffic Direction System
VB2011 - the 21st Virus Bulletin International
Detecting TDS

Synthetic
Detecting TDS

http://domain.com/path

Web Server Structure

Synthetic
Detecting TDS

http://domain.com/path

Web Server Structure

Known File Names

README.txt Version.TXT

TDS Traffic Direction System
VB2011 - the 21st Virus Bulletin International
Detecting TDS

Synthetic

Web Server Structure

Known File Names

Known Folder Names

http://domain.com/path

/config/ /logs/ /temp

README.txt Version.TXT
Detecting TDS

- Synthetic
- Web Server Structure
  - /config/
  - /logs/
  - /temp
- Known File Names
- Known Folder Names
- Variable Names
- README.txt
- Version.TXT
- GET /go.php?q=1
## Statistics: Top 25 Hosts

<table>
<thead>
<tr>
<th>Host</th>
<th>Number of counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>ranks1.apserver.net</td>
<td>810803</td>
</tr>
<tr>
<td>tr-af.com</td>
<td>14293</td>
</tr>
<tr>
<td>cloudaway.com</td>
<td>14260</td>
</tr>
<tr>
<td>0930sb.ranks1.apserver.net</td>
<td>11057</td>
</tr>
<tr>
<td>lxtraffic.com</td>
<td>8358</td>
</tr>
<tr>
<td>webmail.bluewin.ch</td>
<td>7726</td>
</tr>
<tr>
<td>p8238.adskape.ru</td>
<td>6942</td>
</tr>
<tr>
<td>houmekredit.ru</td>
<td>5858</td>
</tr>
<tr>
<td>h46r.com</td>
<td>5477</td>
</tr>
<tr>
<td><a href="http://www.picter.jp">www.picter.jp</a></td>
<td>5121</td>
</tr>
<tr>
<td><a href="http://www.highqualitysearch.com">www.highqualitysearch.com</a></td>
<td>4763</td>
</tr>
<tr>
<td>p103705.adskape.ru</td>
<td>4260</td>
</tr>
<tr>
<td><a href="http://www.japanesegirlfucked.com">www.japanesegirlfucked.com</a></td>
<td>3967</td>
</tr>
<tr>
<td>home-sd.com</td>
<td>3876</td>
</tr>
<tr>
<td><a href="http://www.servedadbutler.com">www.servedadbutler.com</a></td>
<td>3812</td>
</tr>
<tr>
<td>log3.ziyu.net</td>
<td>3806</td>
</tr>
<tr>
<td>webmail.sso.bluewin.ch</td>
<td>3765</td>
</tr>
<tr>
<td>sexy-tube-site.com</td>
<td>3733</td>
</tr>
<tr>
<td>97.64.112.140</td>
<td>3702</td>
</tr>
<tr>
<td>uniangel.info</td>
<td>3687</td>
</tr>
<tr>
<td><a href="http://www.sublimedirectory.com">www.sublimedirectory.com</a></td>
<td>3662</td>
</tr>
<tr>
<td><a href="http://www.youngerbabes.com">www.youngerbabes.com</a></td>
<td>3509</td>
</tr>
<tr>
<td><a href="http://www.asian1tube.com">www.asian1tube.com</a></td>
<td>3328</td>
</tr>
<tr>
<td>sexonane.ranks1.apserver.net</td>
<td>3324</td>
</tr>
<tr>
<td>log5.ziyu.net</td>
<td>3259</td>
</tr>
</tbody>
</table>
## Statistics: Top 25 Countries

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>407110</td>
</tr>
<tr>
<td>United States</td>
<td>212639</td>
</tr>
<tr>
<td>Netherlands</td>
<td>135929</td>
</tr>
<tr>
<td>N/A</td>
<td>70764</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>24908</td>
</tr>
<tr>
<td>Germany</td>
<td>12199</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>6526</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>2791</td>
</tr>
<tr>
<td>Ukraine</td>
<td>2711</td>
</tr>
<tr>
<td>Switzerland</td>
<td>2471</td>
</tr>
<tr>
<td>Asia/Pacific Region</td>
<td>1787</td>
</tr>
<tr>
<td>Cyprus</td>
<td>1525</td>
</tr>
<tr>
<td>Panama</td>
<td>1191</td>
</tr>
<tr>
<td>Australia</td>
<td>1106</td>
</tr>
<tr>
<td>Virgin Islands, British</td>
<td>933</td>
</tr>
<tr>
<td>Canada</td>
<td>926</td>
</tr>
<tr>
<td>France</td>
<td>917</td>
</tr>
<tr>
<td>Belgium</td>
<td>816</td>
</tr>
<tr>
<td>Latvia</td>
<td>803</td>
</tr>
<tr>
<td>Italy</td>
<td>786</td>
</tr>
<tr>
<td>Sweden</td>
<td>774</td>
</tr>
<tr>
<td>Europe</td>
<td>687</td>
</tr>
<tr>
<td>Romania</td>
<td>661</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>361</td>
</tr>
<tr>
<td>Denmark</td>
<td>241</td>
</tr>
</tbody>
</table>
### Statistics: Top 25 Cities

<table>
<thead>
<tr>
<th>City</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Osaka</td>
<td>394601</td>
</tr>
<tr>
<td>N/A</td>
<td>205146</td>
</tr>
<tr>
<td>Amsterdam</td>
<td>48282</td>
</tr>
<tr>
<td>Ashburn</td>
<td>42893</td>
</tr>
<tr>
<td>Dallas</td>
<td>23455</td>
</tr>
<tr>
<td>Fort Lauderdale</td>
<td>15159</td>
</tr>
<tr>
<td>Providence</td>
<td>13811</td>
</tr>
<tr>
<td>Seattle</td>
<td>13010</td>
</tr>
<tr>
<td>Weehawken</td>
<td>9363</td>
</tr>
<tr>
<td>Miami</td>
<td>8995</td>
</tr>
<tr>
<td>Secaucus</td>
<td>8349</td>
</tr>
<tr>
<td>Sakura</td>
<td>7605</td>
</tr>
<tr>
<td>Atlanta</td>
<td>6400</td>
</tr>
<tr>
<td>Herndon</td>
<td>6281</td>
</tr>
<tr>
<td>Saint Louis</td>
<td>6241</td>
</tr>
<tr>
<td>London</td>
<td>5505</td>
</tr>
<tr>
<td>Scranton</td>
<td>5201</td>
</tr>
<tr>
<td>Waltham</td>
<td>4930</td>
</tr>
<tr>
<td>Houston</td>
<td>4684</td>
</tr>
<tr>
<td>Sayreville</td>
<td>3820</td>
</tr>
<tr>
<td>San Diego</td>
<td>3342</td>
</tr>
<tr>
<td>Moscow</td>
<td>3028</td>
</tr>
<tr>
<td>West Palm Beach</td>
<td>2909</td>
</tr>
<tr>
<td>Rotterdam</td>
<td>2818</td>
</tr>
<tr>
<td>New York</td>
<td>2763</td>
</tr>
<tr>
<td>ISP</td>
<td>Hits</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>SAKURA Internet Inc.</td>
<td>402394</td>
</tr>
<tr>
<td>N/A</td>
<td>267485</td>
</tr>
<tr>
<td>Warp Link GmbH</td>
<td>41813</td>
</tr>
<tr>
<td>Ocom B.V.</td>
<td>26203</td>
</tr>
<tr>
<td>HALDEX</td>
<td>22574</td>
</tr>
<tr>
<td>Real International Business Corp.</td>
<td>13886</td>
</tr>
<tr>
<td>Adelphia</td>
<td>9566</td>
</tr>
<tr>
<td>UUNET Technologies</td>
<td>9521</td>
</tr>
<tr>
<td>Marconi Communications North America</td>
<td>6998</td>
</tr>
<tr>
<td>Beyond The Network Access</td>
<td>6267</td>
</tr>
<tr>
<td>ICG NetAhead</td>
<td>5353</td>
</tr>
<tr>
<td>Saturnus Breedband Internet B.V.</td>
<td>4704</td>
</tr>
<tr>
<td>US Net Incorporated</td>
<td>4669</td>
</tr>
<tr>
<td>Global Net Access, LLC</td>
<td>4495</td>
</tr>
<tr>
<td>Reflected Networks</td>
<td>4440</td>
</tr>
<tr>
<td>Teligent</td>
<td>3418</td>
</tr>
<tr>
<td>WebaZilla, Ltd.</td>
<td>3234</td>
</tr>
<tr>
<td>Interserver</td>
<td>2989</td>
</tr>
<tr>
<td>Syncordia</td>
<td>2901</td>
</tr>
<tr>
<td>Productivity Online</td>
<td>2707</td>
</tr>
<tr>
<td>Swisscom Fixnet AG</td>
<td>2403</td>
</tr>
<tr>
<td>EZZI.NET</td>
<td>2181</td>
</tr>
<tr>
<td>SC My Computer SRL</td>
<td>2028</td>
</tr>
<tr>
<td>Asia Netcom Corporation</td>
<td>1789</td>
</tr>
<tr>
<td>NetTransactions, LLC</td>
<td>1470</td>
</tr>
</tbody>
</table>
Conclusion

Traffic Direction Services

New form of underground business

Really difficult to observe

Mixed with legitimate traffic resale

Challenge AV industry in investigations/sourcing

Combined targeting
Questions?
Thanks!

Maxim Goncharov
TREND MICRO Inc.
Thanks!

Maxim Goncharov
TREND MICRO Inc.
Thanks!

Maxim Goncharov
TREND MICRO Inc.