TREND MICRO™
Securing Your Journey to the Cloud

TRAFFIC DIRECTION SYSTEMS AS MALWARE DISTRIBUTION TOOLS

TrendLabs℠

Maxim Goncharov

A 2011 Trend Micro Research Paper

Abstract

Directing traffic to cash in on referrals is a common and legitimate method of making money on the Internet. It should not, therefore, be surprising for the same to be true in the illegitimate world of cybercrime. So-called traffic direction systems (TDSs) have reached a high level of sophistication. This research paper will show how such systems work, how these are utilized by cybercriminals, and what the security industry can do about this.

First, we will take a look at how TDSs work by looking at HTTP header redirection. Then we will look at and compare how TDSs use iframes and *Flash*-based applications to distribute malware.

Cybercriminals try to maximize the effectiveness of TDSs in order to profit as much as possible from their exploits. This paper will also show how time, region, and installed software influence TDSs by looking at the various tools that are currently available in the market.

Cybercriminals strongly utilize TDSs to determine traffic type, which will aid them in directing users to certain malicious sites and in determining what malicious payloads to execute on particular systems. Some malware may also be the end result of a particular TDS's series of redirections, making it a malware infection vector.

What then can we do as part of the security industry?

TDSs present several challenges with regard to malware sample sourcing and malicious URL detection, as these are capable of detecting the use of security tools and often initiate avoidance tactics. A naïve approach to looking at TDSs may, therefore, result in bogus findings and possible damage to the systems of innocent users. This paper will show how we can protect users by actively detecting and blocking the TDSs they may be entangled in.

Web Traffic

In this research paper, "traffic" refers to high-level activities such as clicking a link but not to low-level traffic that travels through network switches and cables. In other words, it will talk about "web traffic."

Web traffic is usually initiated by users via the use of web browsers. It begins with a click to access a URL. Traffic flow starts with a mouse click, which sends browser information to a server that uses predetermined rules and methods to obtain user browser requests. Based on these rules, the server then decides what action is needed.

Dispatching web traffic is now widely used on the Internet to direct unknowing users to hover over an embedded iframe on a site. The continuous increase of Internet users each year is motivating online shop, gambling site, and botnet owners to take control of users' moves to point them to their sites.

Sample TDS Technical Analysis

Several means to redirect traffic exist, some of which are only used to redirect targeted users of very popular software or applications. However, all web traffic redirection techniques intend to lead unknowing users to a certain site. The following are some of the more well-known web traffic redirection techniques:

- Server-side redirection
- Refresh meta tag and HTTP refresh header redirection
- iframe redirection
- *Flash*-based redirection
- Video redirection
- Simple or complicated TDS redirection

Websites or web servers behave differently based on users' system settings. If a transnational company has several sites, localization servers are identified by the number *l10n* while internationalization servers are identified by the number *i18n.* This means that users first contact some kind of script in the middle and, depending on their web client information, they are redirected to the right sites.

Some sites lead users to different site sections or to totally different sites, depending on certain web client information. A good example of these is a huge corporation's site that points users to the right pages, depending on their systems' language settings, OS types, and browsers.

Figure 1 shows how a huge corporation's site in the middle points users from the main site to localized versions.

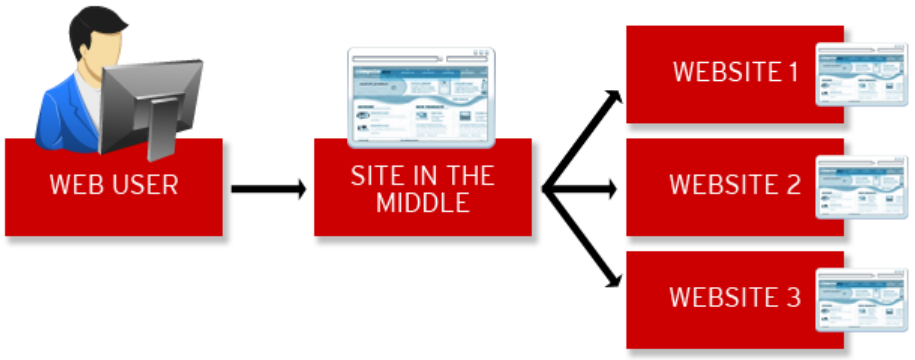

Figure 1. *Site in the middle behavior*

The site in the middle can, however, be more complicated than that shown in Figure 1. It can use additional modules to process user requests based on certain information and to make a multi-optional selection in order to know what server the user should be directed to.

Some sites use more sophisticated methods in order to attract clicks and to direct users to the proper locations via databases and additional interfaces that help control traffic called TDSs (see Figure 2). Databases, redirection gateways, logging information storage devices, and web interfaces control all possible redirection means in TDSs.

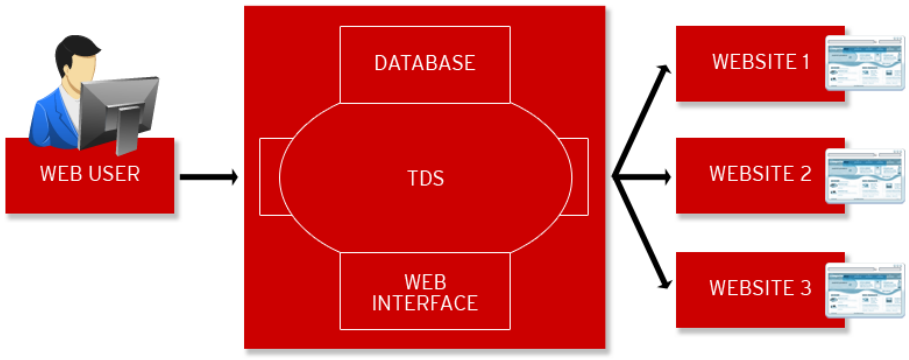

Figure 2. *Structure of sites that use TDSs*

A TDS requires additional file storage devices for logs and web browser functionality components that support *mod_rewrite*-like procedures.

TDSs serve a wide range of functions such as selling pharmaceutical products, exploiting system vulnerabilities using malicious codes, executing SMS games, redirecting unsuspecting users to adult sites, instigating blackhat search engine optimization (SEO) attacks, and others.

TDS Functionality

Traffic Direction

Most of the current known TDS set-ups have almost the same functionality to help their owners control web traffic. A TDS's functions can be categorized into three types—controlling traffic direction, filtering unwanted traffic, and collecting traffic statistics.

Controlling traffic direction is the most important and primary function of a TDS. To control web traffic direction, a TDS can use the dimensions in Figure 3.

```
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-site.com Connection:
Keep-Alive
```

Figure 3. *Dimensions that TDSs use*

The TDS dimensions in Figure 3 have the following components:

1. **Browser (user agent):** This refers to a web browser's version and its equivalent version as delivered by the web agent (browser) to the web server. This information, of course, can easily be spoofed but most Internet users use their browsers as is, making the user-agent information a TDS gathers relevant in most cases.
2. **OS:** This refers to the OS's version and its equivalent version as delivered by the web agent (browser) to the web server.
3. **IP geolocation:** Based on a web agent's IP address, a TDS can easily determine where the user is originally from. Lists of the geographic locations of IP addresses are offered as downloadable databases by various companies. These are primarily used to obtain information on their owners' physical geographic locations. Privately owned companies that collect this kind of information from "open" sources normalize it. They usually offer this data for free or for a minimal fee if it comes with additional information such as each user's region and city as well as daily updates.
4. **Time frame:** This is important so that TDS owners can gauge at what exact times they can monetize user clicks. This parameter is highly used by the owners of adult and pharmaceutical sites. It helps TDS owners determine when each user is most likely to click objects that lead to their sites and to be tempted to buy their bogus products or services.
5. **Referral:** This specifies where a user came from and what referral information filtering application the TDS should use. It controls where a user should be taken to, depending on where he/she originated. Technically, it is used by partner and affiliate programs to calculate how many clicks each particular redirector made.
6. **Web agent local language settings:** These are the most widely used parameters in filtering and directing web traffic for malware distribution, for adult and gambling site redirection, and for other applications. These help TDS owners determine what language a user prefers so he/she can be directed to the proper localized site.

Traffic Filtering

Filtering unwanted traffic is another important functionality that TDS owners use to filter unwanted or dangerous web traffic from their sites or to keep their systems hidden from security companies' search engine crawlers. Traffic filtering is implemented based on the same information used for directing traffic and works in almost the same way. Unlike traffic direction, however, traffic filtering directs most of the unwanted traffic to the most popular sites (see Figure 4).

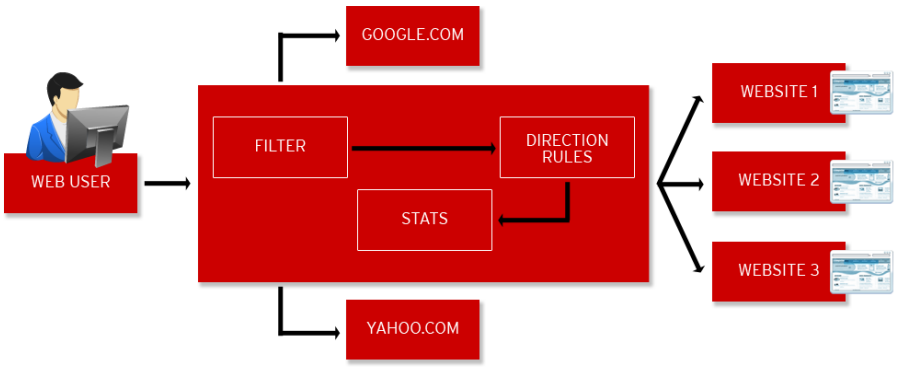

Figure 4. *Traffic filtering functionality's structure.*

Figure 4 shows that web traffic is usually filtered then directed from the very beginning while writing information to a database or a text file at the same time for future statistical means. TDS owners that use the traffic filtering functionality usually redirect unwanted requests to the most popular legitimate sites in order to hide their systems' main function. For example, security companies that scan lists of possibly malicious URLs and IP addresses are filtered by malicious TDS owners to block the HTTP requests of antivirus crawlers. This instead directs security experts to nonmalicious legitimate sites such as *Yahoo!* and *Google*.

Why Site Owners Consider TDSs Instrumental

Every TDS owner primarily wants to direct web traffic without losing it. To do so, they need to use several instruments that were primarily developed to gather and direct traffic to wherever they want (see Figure 5). Most of the software designed for controlling web traffic consists of server-side scripting applications. In some cases, these use databases as storage devices for control rules and for logging information.

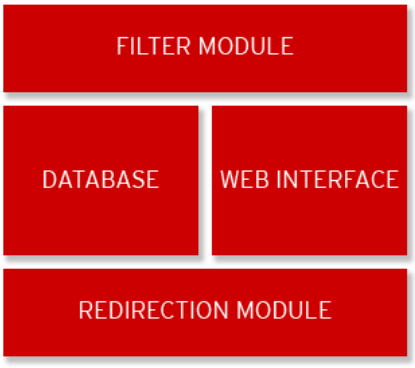

Figure 5. *Additional TDS modules*

IL TDS

IL TDS was developed by the online SEO community known as "FreeIl.net" in 2009. A modified version was released in 2010. *IL TDS* is primarily used in SEO although it has also been used for malware distribution.

Simple TDS

Simple TDS is widely used for SEO as well as for small- and medium-scale pay-per-install (PPI) projects. Many adult or pornographic and online shop sites use it as well. It is interesting to note that *Simple TDS* was developed in late 2008, after which its owner ceased development. Some traffic and SEO activists continued developing concurrent versions using the original code base. Most of the *Simple TDS* versions used for traffic direction nowadays are probably post-development projects.

Sutra TDS

Sutra TDS is currently the most advanced and most powerful TDS software with the ability to process millions of requests per day. It was designed to process a significant number of logs in real time in order to tune up redirection rules. It was developed in 2003 and has been constantly updated since then, hence the stable releases to date. It is unique in that it uses a combination of *FastCGI* and a self-developed *C* code without affecting the infrastructure of its database. As such, it can be deployed on almost any kind of low-end server while still being able to process up to 30 million clicks every 24 hours. It can come with an additional module called *"TS,"* which serves as an interface that emulates traffic market functionality and as a base for partner or affiliate programs. Its and *TS's* code owner also offers additional services for VPN tunneling and for traffic reselling. *Sutra TDS 3.4* is the software's latest version, which is sold for between US$100 and US$130, depending on a buyer's preferred configuration.

Advanced TDS

Advanced TDS has almost the same functionality as *Simple TDS*. However, it also comes with a unique advanced feature—two-layer traffic filtering. Its entire engine was written in *PHP* using *MySQL* as data storage device and requires the use of *Zend Optimizer* for significant server loads. Its development has been discontinued and its current versions are no longer supported, although it is still sold for a 1% share of the total amount of traffic the owner gets.

Kallisto TDS

The most interesting function of *Kallisto TDS* is its ability to hide TDS references using a JavaScript pop-up. It was developed in 2007 and was first sold for US$100 in underground forums. In 2008, its owner made its source code public and stopped further development.

CrazyTDS

CrazyTDS is one of the cheapest TDS solutions priced at US$8.50. Its latest version—*1.3*—was released in March 2010. A new version—*2.0*—is also about to come out. Its functions are similar to most TDS software and support most of the commonly used TDS filtering combinations. It also boasts of a one-click installation process, differentiating it from other available solutions.

Table 1 compares and contrasts the sample TDS software's functionality in greater detail.

Functionality	IL TDS	Simple TDS	Sutra TDS	Advanced TDS	Kallisto TDS	CrazyTDS
Global traffic filtering by HTTP_USER_AGENT and/or HTTP_REFERER	✓	✓	✓	✓	✓	✓
Using direction filters for each URL	✓	✓	✓	✓	✓	✓
Using direction filters for each IP address	×	×	✓	×	×	✓
Using direction filters for each IP-address-URL relationship	✓	✓	✓	✓	✓	×
Using direction filters for each user agent	✓	✓	✓	✓	×	✓
Using direction filters for each geographic location	✓	×	✓	✓	×	✓
Full statistics for hits and URL combinations	✓	✓	✓	×	✓	×
Provisional traffic functionality by share	×	✓	✓	✓	✓	✓
404 traffic handling	✓	✓	✓	×	✓	✓
No user limitations	✓	✓	✓	✓	×	✓
No project limitations	✓	✓	✓	✓	✓	✓
No URL limitations	✓	×	×	✓	✓	✓
Random URL selection inside a project	×	✓	✓	×	×	×
Fast log purging	✓	✓	×	✓	✓	×
Additional module compatibility/application programming interfaces (APIs)	×	×	✓	✓	✓	✓

Table 1. *TDS software's functionality comparison*

Open Source TDSs Versus Zero-Day Exploits and Stolen Traffic

Most TDS programs are open source applications. This means that their source codes can easily be reviewed and analyzed even for undocumented use such as for exploiting zero-day vulnerabilities. How? Figure 6 shows the steps to follow in order to find a TDS, to detect its version, and to gain control of it.

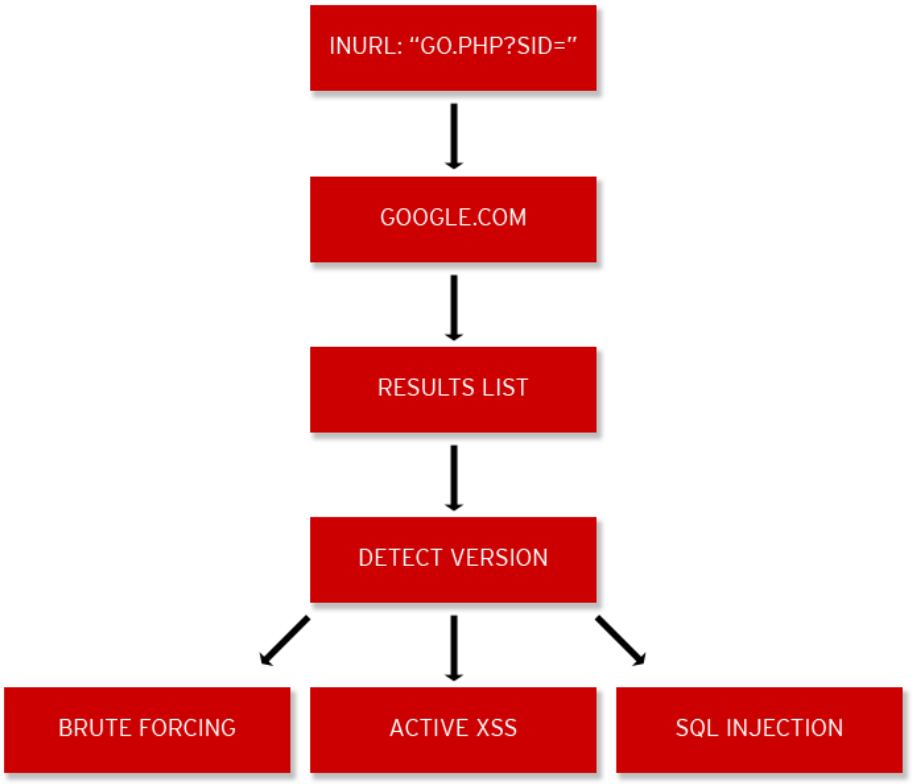

Figure 6. *Steps usually followed to gain control of TDSs*

The example above is based on a compromised traffic direction controller created using one of the most popular pieces of software, *Simple TDS*. Further details of this compromised are provided below.

1. Conduct a *Google* search for the pattern *inurl:"go. php?sid=".*
2. Analyze the results and list all of the sites that possibly use *Simple TDS*.
3. Detect the software version by accessing the *header.php* file in the root folder of the TDS.
4. The version vulnerabilities that can be exploited depend on what *Simple TDS* version a site owner uses.

The steps above are usually followed when compromising TDSs in order to steal statistical data and to hijack traffic from hacked TDSs. These are effectively used to compromise vulnerable TDS software or those with weak passwords and with unlimited server user rights.

Malware Distribution and Iframe Use

Targeted attacks refer to those that prey on certain users, use various social engineering techniques, and utilize specially crafted malware. TDSs have made it possible for cybercriminals to choose either specific targets or wide-ranging groups, depending on their geographic locations, software preferences, and language settings; to deploy and distribute malware; and to steal critical information.

TDSs' traffic filtering and direction control functions allow cybercriminals to select certain possible victims or groups of victims.

Filtering by user agent allows cybercriminals to choose their targets according to their language preferences. The traffic filtering function of TDSs allows them to redirect certain users to malicious landing pages that use their chosen languages. This filtering method is always used in combination with users' geographic locations based on their IP addresses. Different language preferences and geographic locations, however, require localization and internationalization of malicious sites' content.

Filtering by OS and by browser vendor and by their corresponding versions allows cybercriminals to determine what specific vulnerability and exploit kit as well as what exploit code to use. They can, for instance, inject a 0 x 0 iframe on their TDSs, which are capable of handling requests from invisible iframes. To do this, their TDSs should be able to do the following:

1. Handle user requests from legitimate sites that have been compromised via a 0 x 0 iframe injection.
2. Handle users' HTTP requests sent via clicking an invisible iframe.
3. Handle users' HTTP requests that have been initiated, redirected, or pushed by the iframe to the TDS's gateway.
4. Collect browser, OS, referer, and language settings information from the HTTP requests sent to the TDS and combine these with the user's geographical location based on IP address in order to decide where to redirect these.

Provisional Traffic, 404 Requests, and Unintentional Malware Infections

As previously mentioned, provisional traffic can be used to pay for the use of some TDS software for legitimate marketing purposes, for promoting adult sites, for legitimate and blackhat SEO purposes, and for pay-per-click (PPC) as well as PPI schemes.

In the provisional traffic scheme, the total amount of traffic can be shared by the players involved. An adult site owner, for instance, can use *Advanced TDS* to direct traffic to his/her site. To do so, however, he/she needs to pay the software developer 1% of the total amount of traffic as intellectual property fee. If the developer cannot use all of the traffic he/she receives, he/she can resell this in the Partnerka traffic/affiliate program traffic market in order to profit. Traffic brokers then buy and filter traffic before reselling it to PPC business owners. On the other side of the equation, unsuspecting users who click links to the adult site end up with infected systems.

In some cases, highly popular and high-ranking sites make use of 404 requests to nonexistent sites that have been redirected to their servers by selling these in the traffic market. Some of the filtered traffic, unfortunately, ends up on adult sites or on exploit pages. As a result, unsuspecting users' systems are unintentionally infected. Reselling 404 traffic is now becoming a popular trend.

Mixed Traffic and Traffic Market Partnerkas

The traffic that iframes usually redirect comprises a combination of traffic based on browser, OS, referer, language settings, and geographic location. In cases where traffic is not recognized by the TDS, the site owner classifies this as mixed and either tries to sell it to others or to make the best use of it.

The traffic market has several defined sections for particular industries, including the following:

1. **Pharmaceutical:** This industry uses traffic bought to boost sales and to promote new bogus products. It constantly requires and buys traffic, regardless of source. Pharmaceutical site owners filter the traffic they buy based on more specific parameters, for which they use a variety of TDS-like techniques.
2. **Adult:** Like pharmaceutical sites, adult sites require huge amounts of traffic to sell their products or services to. To obtain traffic, adult site owners buy mixed or prefiltered traffic based on the users' regions and language preferences. To maximize profits from the traffic, they further filter it to determine which landing pages each user should be directed to. It is interesting to note that some of the traffic bought from nonadult site marketplaces is filtered by time of day. As such, certain users are directed to pharmaceutical sites during the day but end up on adult sites at night.
3. **PPI:** PPI business owners are known for deploying malicious code and for infecting unsuspecting users' systems. They are paid based on the number of user systems the traffic they sold infected. This means that the better they filter traffic, the more money they earn. They are usually hired by partner or affiliate program members. The number of infected systems is equal to the number of phone-home calls sent to their servers. The infected systems form malicious networks of bots or computer zombies that we know as "botnets."

Conclusion

Directing web traffic has become a new form of online networking business. The increasing amount of web traffic or of the number of user clicks to be directed to the right web pages or sites has given rise to new challenges.

As shown, directing web traffic can be good or bad. It can be good in that when a user clicks a link to a legitimate site, he/she lands on a page on a site that was specifically created for users like him/her in terms of language and the like. It can also be bad in the sense that some users are redirected to malicious pages or sites with a single mouse click.

Security challenges with regard to web traffic direction are becoming clearer and more evident. User redirection to malicious pages or sites has given rise to the importance of understanding TDSs. The possibility of blocking redirection to prevent users from landing on bad sites is thus becoming a valid concern.

The malicious use of TDSs and the practice of leading unknowing users to bad sites is becoming commonplace. Preventing product or service consumers from becoming victims will present the security industry with various technological and financial challenges, as the malicious use of various TDSs will require better sourcing techniques, more advanced detection and blocking tactics, as well as greater manpower to ensure efficiency and effectiveness.