Website analysis project
http://hirado.hu

David SARKOZI
Ecole Polytechnique de Louvain
Université catholique de Louvain
Academic year 2014 – 2015

INTRODUCTION

This report contains the summary of the main technical elements analyzed by interacting with a remote website, namely http://hirado.hu, a hungarian news broadcaster.

1. HTTP ANALYSIS

A. Domain names

![Figure 1. List of domains names, servers and resources summary for http://hirado.hu](image1)

In Figure 1, we can note that for the domain names that belong to the website analyzed¹, there is no Server information in the HTTP response headers. This could have a link with the fact that all the requests are GET requests and there is no special page processing that needs a particular server (it is mainly a static website), or it is perhaps simply because the server used doesn’t retrieve its name to the browser². The other domain names are mainly advertisement providers.

There are also resources of type x-unknown and of size 0 that are probably “fake” resources used for processing-only jobs and are thus not meant to retrieve displayable contents but only process information in a specific kind of way.

In Figure 2, the same kind of information can be obtained, apart from the first domain name, which is actually an IP address (212.40.98.161), and actually provides a video chunk whose content type is video/mp2t. After further digging, I discovered that this video chunk comes from the video player accessible at the top of the website’s page and this player creates several video chunks depending on the video’s loading progression. Those chunks are provided by gamaxmedia.hu, a webvideo content type broadcaster.

B. TCP port numbers

The only port number used is 80 for the website analyzed, as it doesn’t run in HTTPS, mainly because there is no POST request to be carried over encrypted from the user’s web browser and the server.

C. HTTP requests

1) Standard header from homepage: Figure 3 depicts the header lines of the homepage request. It contains standard fields such as the acceptables for the response, the cache controller, the connection state, the cookies contents, the host, the 304 allowor and the browser’s user agent.

![Figure 3. Homepage request header lines.](image2)

2) Non-standard header lines: No non-standard header lines have been found.

---

¹Namely www.hirado.hu, hirado.cms.mtv.hu and hirado.mtv.hu.
²After further digging, it appeared that the server used is nginx.
D. HTTP responses

1) Standard header from homepage: Figure 4 depicts the header lines of the homepage response. It contains standard fields such as the partial content range type support, the age, the connection state, the content information, the date and date it has been modified last. On top of that, there are also several uncommon fields that are described in section I-D2. The version used by the server is HTTP/1.1.

![Figure 4. Homepage response header lines.](image)

2) Non-standard header lines:  

- **X-Adfe: “ads02”**: Retrieved by ad.adverticum.net, this ads website includes an uncommon HTTP response header field and I cannot discover its real use.

- **X-Cache: “cached”**: Specifies the state of the response contents, if it is retrieved from the server’s cache or not.

- **X-Cacheable: “YES”**: Specifies if the response contents is cacheable or not and if not, specifies why.

- **X-Content-Type-Options: “nosniff”**: Mainly used by Google Analytics, this header field is a workaround to prevent Internet Explorer from sniffing the MIME type of the response contents. Content sniffing is determining the type of a file by analysing its contents. It is used mostly by Internet Explorer to display contents correctly even if the content type information isn’t available. But this can lead to serious security issues, so it is often disabled by this mean.

- **X-Pingback: “http://www.hirado.hu/xmlrpc.php”**: Present after a search request, it specifies the file that will handle XML-RPC requests initiated by a pingback. A pingback is used to notify a website that another website links to it. In this case, a search request gives as results a list of links pointing to news containing the keywords searched. Since the results page contains links to news articles, a pingback is issued to make the articles know that this page has links to them.

- **X-Powered-By: “PHP/5.3.3”**: Specifies the technology supporting the website application.

- **X-UA-Compatible: “IE=edge, chrome=1”**: Specifies the preferred rendering engine of the website.

- **X-XSS-Protection: “1; mode=block”**: Cross-site-scripting filter to prevent XSS attacks.

A. hirado.hu

Having only A records, the domain name analyzed is accessible only via one IPv4 address (194.149.26.60) and never changes from one day to another, so there is no form of load balancing. The Name Servers are nsauth.datanet.hu and nsauth3.datanet.hu and the TTL is 3600.

1) **nsauth.datanet.hu**: Accessible only via IPv4 (194.149.0.194), no load balancing and the TTL is 600.

2) **nsauth3.datanet.hu**: Accessible only via IPv4 (195.228.156.32), no load balancing and the TTL is 600.

B. www.hirado.hu

Having only A records, the CNAME is www.mediaklikk.hu and the CNAME is 3600.

1) **www.mediaklikk.hu**: Accessible only via IPv4 and the address and TTL are the same as hirado.hu, no load balancing.

C. ad.adverticum.net

Accessible only via IPv4 (81.0.120.6), no load balancing and the TTL is 600. The Name Servers are ns0.prim.hu and ns1.prim.hu.

1) **ns0.prim.hu**: Accessible only via IPv4 (81.0.120.72), no load balancing and the TTL is 60, so the refresh occurs more often.

2) **ns1.prim.hu**: Accessible only via IPv4 (212.52.167.142), no load balancing and the TTL is 60, so the refresh occurs more often.

D. hirado.cms.mtv.hu

Having only A records, the CNAME is hirado.mtv.hu, the TTL is 300 and the IP address is the same as hirado.hu, no load balancing. The Name Servers are ns1.mtv.hu and ns1.prim.hu.

1) **ns1.mtv.hu**: Accessible only via IPv4 (194.149.26.9), no load balancing and the TTL is 300.

2) **ns1.prim.hu**: Accessible only via IPv4 (195.56.77.76), no load balancing and the TTL is 86400 (1 day). We can note that t-online.hu also appears in another Name Server ans0.t-online.hu but that one does not have records of hirado.mtv.hu.

3) **ans2.telekom.hu**: Accessible only via IPv4 (193.225.4.82), no load balancing and the TTL is 86400. We can note that telekom.hu also appears in the Name Servers of t-online.hu, and although I know that Telekom and T-Online are from the same joint stock company (Magyar Telekom), after further digging, it appeared that despite the two websites being identical, the IPv4 addresses differ (telekom.hu: 84.2.36.220 and t-online.hu: 84.2.36.211).

Conclusion

After the whole DNS analysis, it appeared that hirado.hu and all the domains linked with it only have A records and perhaps is not suited to accept IPv6-only systems.

---

III. TCP ANALYSIS

A. TCP options

- **Window size scaling factor**: 128 from the browser, 256 from the server.
- **Selective acknowledgments**: Permitted
- **Timestamp value**: Sent in each TCP SYN packets
- **Timestamp echo reply**: Set to 0 in TCP SYN packets, it can be retrieved from ACK packets.
- **Maximum segment size**: 1380

B. TCP connection termination

All the TCP connections initiated with a SYN-ACK three-way handshake terminated with a FIN flag.

CONCLUSION

With this analysis, I managed to evaluate how hirado.hu, a hungarian news broadcaster, works in terms of HTTP, DNS and TCP. It appears to be a relatively static website holding only A (IPv4) records and having no HTTPS connection perhaps because of the lack of POST requests and server-side processing. It has though a pingback functionality when executing a search query.