ZENK-SECURITY

Tracer un Flux Vidéo

Ou comment remonter à la source d'une vidéo...

Sophocle 10/10/2011

• Tracer une Vidéo Daylimotion

Daylimotion est un site web permettant de lire des vidéos en streaming directement depuis ce dernier. Mais quelques fois, par soucis de facilité, certaines personnes préfèrent – lorsqu'une telle option est disponible – télécharger la vidéo plutôt que d'être obligé de se connecter à chaque fois sur un serveur uniquement pour la visualiser.

Ce document a été écrit dans ce but, et pour cette démonstration, je vais vous montrer comment avec un simple analyseur réseau (Wireshark, Ethereal...) et un navigateur (Firefox, IE, Opera...) il est possible de remonter la source d'un signal vidéo reçu sur des sites comme Daylimotion, Youtube, ARTE...

Pour cette étude, je vais choisir comme vidéo « L'histoire interdite du piratage informatique 1.3 ».



À partir de là, on lance une analyse réseau et on cherche tout simplement à obtenir la source du flux vidéo, qui au passage est au format MP4 sur ce site.

😋 (Untitled) - Ethereal	- 8 ×						
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp							
▋▓ ▋\$	🍑 🗹 👪 🔆 🔯						
Eilter: (ip.addr eq 192.168.0.12 and ip.addr eq 195.8.214.59) and (top.p 🔻 Expression Clear Apply							
No. Time Source Destination Protocol Info							
548 50.051358 192.168.0.12 proxy-59.ix.dailym TCP 1680 > http [SYN] Seq=0 Ack=0 win=16384 555 50.146744 proxy-59.ix.dailym 192.168.0.12 TCP http > 1680 [SYN, ACK] Seq=0 Ack=1 win= 556 50.146812 192.168.0.12 proxy-59.ix.dailym TCP 1680 > http [ACK] Seq=1 Ack=1 win=17520 558 50.148371 192.168.0.12 proxy-59.ix.dailym HTTP GET /video/605/312/22213506 mp4 h264 aa	Len=0 MSS=1460 5840 Len=0 MSS=1460 Len=0 c.mp42auth=1318288840.b						
562 50.209122 proxy-59.ix.dailym 192.168.0.12 TCP http > 1680 [ACK] seq=1 Ack=909 Win=726 575 50.341373 proxy-59.ix.dailym 192.168.0.12 HTTP HTTP/1.0 200 OK (video/mp4) 577 50.381870 proxy-59.ix.dailym 192.168.0.12 HTTP Continuation or non-HTTP traffic	4 Len=0						
578 5 @ Follow TCP stream 579 5	20 Len=0						
<pre>S80 5 S80 5 S80 5 S80 5 S81 5 S82 5 Host: proxy-59.dailymotion.com User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; fr; rv:1.9.2.10) Gecko/20100914 Fir. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 115 Connection: keep-alive Cookie: oAX=VkUDYU6PerMACgxk; nextp_1_5=0; nextp_0_9=1; nextp=0; cto_dailymotion=/criteo Frame Frame Frame Hypert HTTP/1.0 200 OK HTTP/1.0</pre>	- 520 Len=0 520 Len=0 520 Len=0 7520 Len=0 3.214.59)						
Last-Modified: Fri, 22 Jul 2011 19:30:33 GMT Content-Length: 67599211 Connection: close Content-Type: video/mp4 ftypisomisomiso2avc1mp41moovlmvhd % 0040 2f 0050 36 0070 34 Save As Print Entire conversation (199468 bytes) Save As Print Entire conversation (199468 bytes) Filter out this stream Close Filter out this stream Close							
0.0c0 65 File: (Untitled) 423 KB 00:01:05 [P: 863 D: 235 M: 0 Drops: 0							
🧑 💌 🖏 🔏 » 🖏 Zenk-Tracer un Flux 関 Dailymotion - L'hist 🍘 (Untitled) - Ethereal 🎯 Ethereal: Capture In 🙆 🔳 🔐	T 10 - 2 P) '9, (0) 5 23:22						

Je disais donc, on lance son sniffeur préféré (Ethereal pour la démo), on lance une capture réseau, on recharge sa page Daylimotion (afin de relancer une requête HTTP sur la source d'origine), on place un filtre sur la transaction via un petit « Follow TCP Stream » [Clic Droit], et on obtient l'écran ci-dessus.

On retrouve bel et bien l'hôte cible (un Reverse Proxy de prime abord...), et le fichier source en MP4. Une fois remis en forme, on obtient l'URL d'origine du fichier qu'il suffit juste de copier dans la barre d'adresse (F6), soit « proxy-59.dailymotion.com/video/605/312/22213506_mp4_h264_aac.mp4?auth=13 18288840.b97014cbc88f70453b03c6b1d6b7ecb5 ».

Ce qui nous donne finalement avec Firefox ...



Cet exemple était très simpliste et se base sur HTTP, mais d'autres sites comme ARTE, utilise le protocole RTMP et quelques crytages, il vaut donc mieux utiliser RTMP Dump par facilité.

• Tracer une Vidéo ARTE

À présent que les bases sont posées, nous allons découvrir que certains sites internet se défendent plutôt pas mal contre ce genre de menace (qui au passage, peut être assimilé à un viol de Copyright !!).

Bien, on commence par ce que nous connaissons : le sniffing. Mécaniquement vous allez vous dire « On a qu'à exécuter un GET sur la page affichant la vidéo, capturer le traffic via Ethereal/Wireshark, remonter l'origine du flux dans le logiciel, et sauvegarder avec le navigateur... ». OK essayons !!

Je choisi comme source vidéo « La Guerre Invisible ½ » disponible sur http://videos.arte.tv/fr/videos/la_guerre_invisible_extrait_1_2_-3952072.html



On lance la requête, on sniff les trames réseaux, et on observe tranquillement le résultat...

Elle Edit Yiew Go Capture Analyze Statistics Help Image: Statistics Mail Image: Statistics Help Image: Statistics Help Image: Statistics Image: Statistics Help Image: Statistics Help Image: Statistics Help Image: Statistics Image: Statis
Image: Source Destination Protocol Info 13 0.158703 192.168.2.14 62.161.94.221 Protocol Info 19 0.221868 91.213.146.11 192.168.2.14 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmar di%3A%3A3950' 19 0.221868 91.213.146.11 192.168.2.14 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmar di%3A%3A3950' 249 2.877906 192.168.2.14 91.213.146.11 192.168.2.14 503 5.161869 192.168.2.14 91.213.146.11 HTTP 62.161.94.221 192.168.2.14 HTTP HTTP HTTP/1.1 200 OK (GIF89a) 503 5.161869 192.168.2.14 HTTP HTTP HTTP/1.1 200 OK (GIF89a) 503 5.161869 192.168.2.14 HTTP HTTP/1.1 200 OK (GIF89a) 1024&sch=76&scscp=24&rs 503 5.161869 192.168.2.14 HTTP HTTP/1.1 200 OK (GIF89a) 1024&sch=76&scscp=24&rs 514 5.238155 62.161.94.221 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmar di%3A%3A3950' 514 5.238155 62.161.94.221
Filter: Expression Glear Apply No. Time Source Destination Protocol. Info 13 0.158703 192.168.2.14 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 19 0.221868 91.213.146.11 192.168.2.14 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 249 2.877906 192.168.2.14 91.213.146.11 HTTP HTTP 260 2.971850 91.213.146.11 192.168.2.14 HTTP GET /m/web/277077202316?n=6003461569&scw=1024&sch=768&scp=24&r 260 2.971850 91.213.146.11 192.168.2.14 HTTP HTTP GET /m/web/277077202316?n=6003461569&scw=1024&sch=768&scp=24&r 260 2.971850 91.213.146.11 192.168.2.14 HTTP GET /m/web/277077202316?n=6003461569&scw=1024&sch=768&scp=24&r 260 2.971850 91.213.146.11 192.168.2.14 HTTP GET /m/web/277077202316?n=6003461569&scw=1024&sch=768&scp=24&r 503 5.161869 192.168.2.14 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 514 5.238155 62.161.94.221
No. Time Source Destination Protocol. Info 13 0.158703 192.168.2.14 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 19 0.221868 91.213.146.11 192.168.2.14 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 23 0.310327 62.161.94.221 192.168.2.14 HTTP HTTP/L.1 200 oK (GIF89a) 249 2.877906 192.168.2.14 91.213.146.11 HTTP GET 260 2.971850 91.213.146.11 192.168.2.14 HTTP HTTP 260 2.971850 91.213.146.11 192.168.2.14 HTTP HTTP 260 2.971850 91.213.146.11 192.168.2.14 HTTP HTTP/1.1 200 oK (GIF89a) 503 5.161869 192.168.2.14 62.161.94.221 HTTP GET 514 5.238155 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 514 5.238155 62.161.94.221 HTTP
10 0.117155 192.168.2.14 0.1115.11 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 13 0.158703 192.168.2.14 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 19 0.221868 91.213.146.11 192.168.2.14 HTTP HTTP HTTP/1.1 200 oK (GIF89a) 249 2.877906 192.168.2.14 91.213.146.11 HTTP GET /m/web/277077202316?n=6003461569&scw=1024&sch=768&scp=24&r 260 2.971850 91.213.146.11 192.168.2.14 HTTP GET /m/web/277077202316?n=6003461569&scw=1024&sch=768&scp=24&r 260 2.971850 91.213.146.11 192.168.2.14 HTTP HTTP GET /mix.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 503 5.161869 192.168.2.14 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 514 5.238155 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 514 5.238155 62.161.94.221 192.168.2.14 HTTP HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' Samada Sama
859 10.355253 62.161.94.221 192.168.2.14 HTTP HTTP/1.1 200 ok (GIF89a) 1133 15.170722 192.168.2.14 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 1144 15.325871 62.161.94.221 192.168.2.14 HTTP HTTP/1.1 200 ok (GIF89a) 1368 20.155415 192.168.2.14 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 1369 20.214846 62.161.94.221 192.168.2.14 HTTP HTTP/1.1 200 ok (GIF89a) 10.0000000 192.168.2.14 62.161.94.221 HTTP GET /hit.xiti?p=videothek%3A%3A602thema%5Fdu%5Fmardi%3A%3A3950' 11368 20.155415 192.168.2.14 62.161.94.221 HTTP HTTP/1.1 200 ok (GIF89a) 10.0000000 192.168.2.14 HTTP HTTP/1.1 200 ok (GIF89a) 1100.000000 192.168.2.14 HTTP HTTP/1.1 200 ok (GIF89a) 1100.000000 192.168.2.14 SLV2 1200 ok (GIF89a) 10.000000 192.168.2.14 1200 ok (GIF89a) 10.000000 192.168.2.14 SLV2 Encrypted Data, [Unreassembled Packet] 9 0.104367 fcds104.par.11nw.n 192.168.2.14 SLV2 Encrypted Data, Encrypted Data, [Unreassembled Packet] 9 0.104367 fcds104.par.11nw.n 1
[Unreassembled Packet: SSL] 0000 9a 17 33 e9 30 ad 00 e0 4c 9d d8 49 08 00 45 00 3.0 L.I.E. 0010 00 49 b9 a7 40 00 80 06 49 14 c0 a8 02 0e 57 f8 II.@ Iw. 0020 dd 44 0e 6d 01 bb 3f c5 99 40 6d a6 a7 e5 50 18 .D.m.?. @mP. 0030 42 99 4f 7a 00 00 88 01 51 0c 02 00 05 70 61 75 B.OZ Qpau 0040 73 65 00 00 00 00 00 00 00 00 05 01 00 00 40 se@ 0050 f0 4c 80 00 00 00 00 050
File: (Untitled) 1448 KB 00:00:24 P: 1689 D: 1689 M: 0 Drops: 0

Oh mince... Que vois-je ?! Un Cryptage SSLv2 !! Et oui, comme dit plus haut, certains sites utilisent quelques techniques simples mais très efficaces pour se protéger. Le fonctionnement pourrait être le suivant :

- Le navigateur télécharge le lecteur vidéo propriétaire du site
- Le player télécharge petit à petit la vidéo en cryptant la liaison avec le serveur (via SSL)
- Le player décrypte à la volé, et affiche à l'écran

Mais réfléchissons, SSL permet de protéger les données qui transitent sur un réseau, par sur un système. Donc de l'autre côté, comme du notre au travers du Player, le fichier est en clair !! Regardons un peu la source.



Un petit [CTRL+U], suivit d'une recherche sur le mot clé « SWF », et on tombe sur la plage de code gérant l'affichage de la vidéo sur la page. En y regardant de plus près, on trouve une variable intéressante : « videorefFileUrl ».

On Copie-Colle cet URL dans Firefox (après l'avoir remis en forme), et on observe quelque chose d'intéressant : Un fichier XML plein d'informations !!



Aucune information de style ne semble associée à ce fichier XML. L'arbre du document est affiché ci-dessous.



Terminé			
🕑 🗷 🖉) 💪 🚿 📑 Zenk-Tracer un Flux Vid	👌 Mozilla Firefox	💵 🗐 🗐 🏷 - 03:50

Ce fichier source XML contient un lien vers un autre fichier XML « ligne 6 ». Et en affichant ce dernier fichier avec son navigateur, on obtient l'origine du flux vidéo, et en clair qui plus est !!

Bien entendu, le Hack ne s'arrête pas ici, essayez d'ouvrir un protocole RTMP avec Firefox, vous verrez...



Maintenant que nous connaissons l'origine exacte du flux, il nous suffit d'en faire une copie sur Disque. Mais il faut en premier lieu le récupérer. Et pour ce faire, il existe un outil : RTMP Dump. C'est un programme portable et open-source disponible à l'adresse fournit en bas de document.

On ouvre son Invite de Commande favorite, on se place dans le répertoire de RTMP Dump, et on a plus qu'à télécharger gentiment .

Commande : rtmpdump -r

rtmp://artestras.fcod.llnwd.net/a3903/o35/mp4:geo/videothek/ALL/artepro d/2011/06/03/ARTE3952072_FR_112073_16by9_300_MP4?h=67731ea6c41d 6e71cc2c5df807d92432 -o Ma_Video.flv

L'extension FLV est qui plus est une erreur car c'est du MP4... Pas grave.

🔤 C:\WINDOWS\system32\cmd.exe - rtmpdump -r rtmp://artestras.fcod.llnwd.net/a3903/o35/mp4:geo/videothek/A... 💶 🗗 🗙 deothek/ALL/arteprod/2011/06/03/ARTE3952072_FR_112073_16by9_300_MP4?h=67731ea6c4 1d6e71cc2c5df807d92432 -o Ma_video.flv RTMPDump v2.3 (c) 2010 Andrej Stepanchuk, Howard Chu, The Flustreamer Team; license: GPL Connecting ... Caught signal: 2, cleaning up, just a second... ERROR: RTMP_Connect0, failed to connect socket. 10060 (Unknown error) C:\rtmpdump-2.3>rtmpdump -r rtmp://artestras.fcod.llnwd.net/a3903/o35/mp4:geo/vi deothek/ALL/arteprod/2011/06/03/ARTE3952072_FR_112073_16by9_300_MP4?h=67731ea6c4 1d6e71cc2c5df807d92432 -o Ma_video.flv RTMPDump v2.3 (c) 2010 Andrej Stepanchuk, Howard Chu, The Flvstreamer Team; license: GPL Connecting ... WARNING: HandShake: client signature does not match! INFO: Connected... ERROR: HandleCtrl: Ignoring SWFVerification request, use ---swfVfy! Starting download at: 0.000 kB INFO: Metadata: INFO: INFO: duration moovPosition $164.72 \\ 32.00$ 32.00 mp4a 384.00 216.00 avc1 77.00 13.00 2.00 44100.00 2.00 INFO: INFO: INFO: INFO: INFO: INFO: INFO: audiocodecid width height videocodecid avcprofile avclevel NFO: aacaot NFO: audiosamplerate NFO: audiochannels NFO: videoframerate NFO: trackinfo: 2.00 INFO: INFO: length 7264256.00 timescale 44100.00 INFO: Language INFO: sampledescription: INFO: sampletype INFO: length INFO: timescale eng mp4a 4114000.00 25000.00 INFO: language eng NFO: sampledescription: sampletype length NFO: avc1 7265280.00 44100.00 NFO: NFO: NFO: timescale language und NFO: sampledescription: NFO: length 14810400.00 90000.00 INFO: length INFO: timescale INFO: language INFO: sampledescription: INFO: length INFO: timescale INFO: language und 7265280.00 44100.00 language und INFO: sampledescription: NFO: length 14810400.00 NFO: 90000.00 timescale NFO: language und NFO: sampledescription: 57.680 kB / 1.16 sec (0.7%) NFO:

Outils

Wireshark : http://www.wireshark.org/download.html

<u>RTMP Dump</u> : <u>http://rtmpdump.mplayerhq.hu/download</u>

WinPCAP : http://www.winpcap.org/install/default.htm

Amusez-vous bien ;)