

Backdooring QuickTime Movies

Backdooring QuickTime Movies - pdp, GNUCITIZEN.

- Published: 2006-09-05
- Original: <<https://www.gnucitizen.org/blog/backdooring-quicktime-movies/>>
- Preserved from: <https://www.gnucitizen.org/blog/backdooring-quicktime-movies/> (manual-import) on 2026-09-10
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Backdooring QuickTime Movies

September 5th, 2006

[Original lead illustration: kodo_ipod.jpg](#) — image not recovered

XSS attacks are nothing new, but an evil mind can find ways to use these flows to bypass border firewalls and highly expensive intrusion prevention systems in order to attack your organization from inside.

This post outlines an example of how to use QuickTime Movie files to trick the user into executing malicious JavaScript code. The technique presented here does not relay on a vulnerability but rather on an insecure feature present in QuickTime player from version 3, up to the latest version 7.

This technique makes use of one of the very well know features in QuickTime called Text Tracks. Movie files are usually constructed of video and audio tracks. They provide the auditory and visual characteristics of the movie. On the top of them Text Tracks enable subtitles, lyrics and other very interesting and highly productive accessibility features.

One layer bellow, Text Tracks can be of different types. There are many of them but the ones that are the most interesting are called HREF Tracks. HREF Tracks contain links that will be opened automatically or when the user clicks on the movie frame. These links can point to URLs from the FTP/HTTP/HTTPS space and also other supported protocols such as the JavaScript protocol (javascript:). Effectively, this feature can be used by attackers to hide malicious code inside a .mov file which will be executed automatically on preview.

HREF Tracks can be created with QuickTime Pro and probably other .mov editors and publishers. I wasn't able to find any command line tools although while researching, several good opensource

QuickTime editing libraries were encountered. The following post examines the process of creating backdoored .mov file with QuickTime Pro.

The first stage is the create a Text Track. Text Tracks are simple .txt files that contain special syntax. For the purpose of this proof of concept I composed the following track named (backdoor.txt).

```
A<javascript:alert("hello from backdoor")> T<>
```

Obviously the code above will display an alert box. The prefix A defines that the action will be automatic - no user interaction is required. There is also T flag, which specifies the target for the action. In this case it is null.

The next stage is to open both backdoor.txt and the movie that will be backdoored with QuickTime Pro. I chose Sample.mov. This is standard movie file that is supplied with every default QuickTime installation.

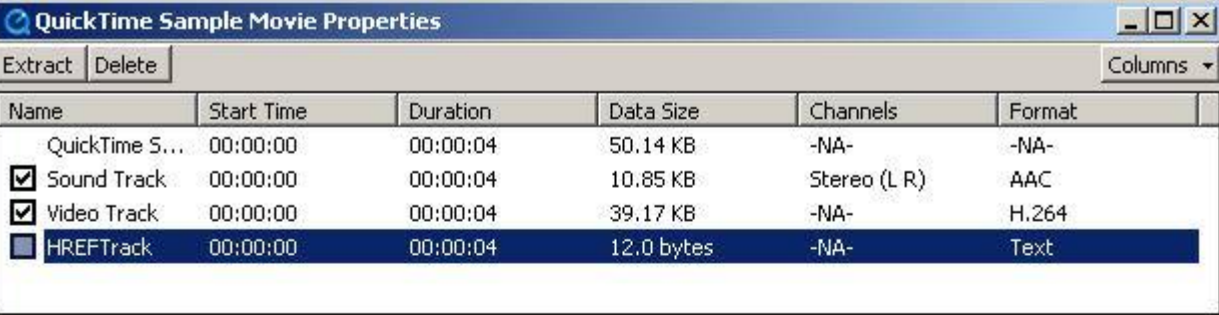
Once opened select the tack file and click on Edit -> Select All. This will select the entire track. Than you need to copy it by going to Edit -> Copy.



The next stage is obviously pasting. Select Sample.mov and click on Edit -> Select All and than Edit -> Add to Selection and Scale. After performing this action you will see that part of Sample.mov frame is covered in black with text inside. This is the Text Track.



Once the Text Track is there, it has to be converted to HREF Track. Select Sample.mov window and click on Window -> Show Movie Properties. In the Movie Properties dialog select "Text Track" and untick the check box next to the label. The last stage is to change the name of "Text Track" to "HREFTrack". Figure this out yourself :).



The produced file will popup an alert box when opened in the browser window. There is no need to discuss again why this is dangerous and in what ways it can be used to bring havoc and destruction. The important bit is to never trust anything from the web. Movie trailers should not be previewed unless they come from apple.com. Don't open audio files or anything that ends with .mov. This is my advice.

comments

Good job pdp! I like the concept of XSS through the backdooring of media files. Everyone likes media files, so it's an ideal way to exploit both human and technical weaknesses.

Imagine downloading Michael's Jackson Thriller video clip which exploits your router's web interface in order to expose internal hosts to the Internet :D

Nice one!

Alberto responds:

I'm probably posting a real newbie question, but I've opened both files you provided with QuickTime Alternative codecs (with VLC and Media Player Classic) and I can't see any difference or pop-up. It is just silently failing but still vulnerable or this codec (Quicktime 7.0.4) is safer to use?

pdp responds:

The example backdoor will work only if the movie file is embedded inside a page or previewed inside the browser.

However, it is possible to make a movie that is previewed inside a standalone QuickTime player to open a remote page which in turn can contain malicious code. Of course this is not very stealthy but can be successfully used to attack the browser at a very low level.

I haven't tested opening URLs with VLC and Media Player Classic. However, if both players support HREFTracks, then they are affected by this issue.

nrg responds:

@Alberto You have to open in a program that can interpret javascript. Like a web browser. just click in the video link to see it in your browser.

- @pdp once again good job mate

lolage responds:

"if both players support HREFTracks, then they are affected by this issue." - Now you're assuming my friend. Although nice find, great work.

pdp responds:

I wish I have more time to play with that. But, yeh... well said.

Chris responds:

Isn't this already widely used on Gnutella? There is a lot of .mov spam, usually pr0n but also for other sites, which will open certain links in a browser window. I don't think these use JavaScript though.

pdp responds:

Chris,

you might be right. I am not sure. Several readers verified that some video formats are able to open links in the browser. It will be good if someone verifies all that.

smetten responds:

Hi all,

This seems to be very interesting information. I'll be having a good look at this, might come in handy some time.

Greetz

Smetten

... responds:

jesus, you made me spend like 10 minutes looking for a way to rename the text track to HREFtrack :) anyone else who wants to do this, just single click on the text track name and you can edit it

Loucas responds:

Hi thanks for the example. I would like to know if is possible to create the popup alter when the movie is previewed inside a standalone QuickTime player.

pdp responds:

IMHO I don't think it is possible. What ever you do, it will be opened in a browser window. However, don't take my word for granted.

Have you seen any .mov files that open pop-up boxes rather than full browser windows? If yes, it will be easy to decompose that and see what is going on.

mcamis responds:

im bored dont block the website i should be in class but i want MYSPACIA!!!!!!!!!!!!!!

SINCERLY

BORED_001

mistersquid responds:

I've loaded the Sample_backdoored.mov in my web browser (Safari 2.0.4) with OS X 10.4.8 (Security Update 2006-07) and I'm not getting any pop-ups.

I'm running QuickTime 7.1.3 but not QuickTime Pro.

This proof-of-concept seems to be a non-starter.

pdp responds:

Hello mistersqui, unfortunately I am not running MacOS. However, here from my side it works. If somebody is willing to investigate on that matter, please you are more than welcome.

I don't think that Apple has fixed this issue and I am not sure if they will because the exploit presented in this article depends on a feature rather than a bug. Many thanks.

ohemia responds:

I agree with mistersquid - no popup here on MacOS X. Doesn't seem to work at all on the Mac.

Jeffbart responds:

Not getting popup either. Also running Safari 2.0.4. Not installed latest security updates. OS X 10.4.8.

Anton responds:

The demonstration works in FireFox 2.0 on Mac OS X 10.4.8. It does not work with Safari.

I'm not sure why. Apple's QT documentation claims only that JavaScript functions defined on the same web page as the movie can be invoked, so perhaps Safari is adhering more strictly to this specification.

BdcstTek responds:

Mac OSX, Version 10.4.6, without the latest security update...(probably without a few)

Safari v 2.0.3 is not affected: no popup window

Firefox v 1.5.0.8 IS affected, and Backdoor did indeed say hi.

Which goes along with the way Safari seems to "Think Different" with JS a bit too much.

pdp responds:

I guess it is all clear now. Safari complies with Apple's specifications while Firefox and IE don't. There must be something wrong with QuickTime browser integration.

Wladimir Palant responds:

What I fail to see here is the XSS part of it. It is bad of course that a movie can load web content through the browser (why did they chose to do this instead of connecting directly from the plugin???) but any JavaScript is still executed in the context of the web page. This means that it will only be able to do something the web page itself can do, so that anybody able to put a movie into a web page could do the same by directly putting the necessary JavaScript code into it. Unless of course it is used somewhere where JavaScript is filtered out but movies are allowed - is it what happened on MySpace?

pdp responds:

exactly!

Brennan Young responds:

This isn't a backdoor. It's a sloppily coded website. The same sh1t can happen with SWFs and DCRs.

HREF tracks have been around for about 10 years, with all this functionality. This page is worth a look, especially the last section "More on QuickTime and HREFs.":

<http://www.apple.com/quicktime.....racks.html>

Scarcely news, but it's great if you guys see some more of what QuickTime can do, even if you all have dastardly plans. ;)

The page linked above also shows how a MOV can open any QuickTime viewable file in another window *in QuickTime player itself*, if you wanted to make a little grey-goo / denial of service beastie.

There's also a turing-complete bytecode interpreter built-in to QuickTime. Apple usually forgets to mention it because it doesn't help to sell iPods.

<http://developer.apple.com/doc.....dIntro.htm>

So, if you're feeling particularly dastardly your MOV could even construct javascript URLs on the fly.

pdp responds:

Hi Brennan,

yes you are completely right. However, It is the same situation with everything in the computer security field. Look at BF attacks, for example. We have been knowing about them since the 80s.

Still, people find clever ways to inject instructions into remote and local processes.

I am sure that HREF tracks is nothing new to core QuickTime/Apple developers. However, the problem is that they wasn't able to spot this potential misuse of their technology. It is not their fault. At the time when this technology was designed, I don't think that anyone was familiar with XSS to that extend as we are today. This problem is so common and I am sure we will see more of it very soon.

Additional comments preserved by the author's later site

Archive note: The following 23 later comments follow the original thread in the author's current page. The article and preceding comments above retain the 2006 capture's wording.

Richard John

Hmm... When I try and rename Text Track to HREFTrack, I change the name and it changes back as soon as I hit enter!

pdp

Richard, that's not supposed to happen. You are sure that you do it properly. The GUI is a bit bulky.

ConcernedUser

Hi. I was wondering is there any way to check the existing mov files that I have if they have any href tracks in them. I do not have quicktime pro. Also, how can u detect that a mov file in your browser might have a malicious href track before playing it?

pdp

ConcernedUser, I am not aware of any tools that you can use. It will be good if someone can come up with Firefox extension, but this probably wont happen. The best thing to so is to wait for a fix from Adobe. Actually there is one that is offered to MySpace users only on Windows platform. If you happen to be on Window, go to MySpace an try to open .mov file that someone has hosted. Then you will receive the update. There are other solutions but they are all unofficial and they might work only in certain situations. Good luck. I hope Apple understands that this is a serious security issue and it requires immediate actions.

psyc

Hmm... When I try and rename Text Track to HREFTrack, I change the name and it changes back as soon as I hit enter! Yea same problem with me ..

pdp

Well, this is the tricky bit. You need to show your creative mind here. The reast is easy :)

psyc

Heh forget about it, i always love reverse engineering ;) Problem solved

Edward

I couldn't change the name to HREFTrack too, i searched forums and heard that it's QT 7 bug. How can we change it ? Found some scripts to change but i don't know how to use. Can someone help please ?

AR

If you can't change it, you most likely need to update Quicktime. It is a bug in the one version that does not allow you to change it.

Nick

How do you pop the browser directly from quicktime standalone player? I can make it work from within the browser, but I want it to pop directly from the stand alone player.

pdp

I am not quite sure how to do that but I know that it is possible since I did it before. Try to mess with the target field

```
A<javascript:alert("hello from backdoor")> T<target>
```

Windows Vista

neat

lastjedi

i have quicktime pro and vlc media player none work on limewire.when i download a video to watch i get the same thing a girl dancing for about 10 seconds nothing else.ive downloaded hundreds of videos and i get the same thing the girl dancing.why wont it show the video i downloaded.nothing works please help!

Cityboi

How can you get around websense to get to myspace

sasha

How can you get around websense to get to myspace

Runic

Starting with QuickTime 7.1.5, you can no longer issue javascript:// URLs or call JavaScript functions from within a QuickTime movie. This feature was removed from QuickTime for security reasons.

pdp

yes... this is right... and this is how it should be

dodgescabin

I never use quicktime its not very good

Doc

Quote [dodgescabin responds: I never use quicktime its not very good] ??? What the f**? - Is that the dumbest sweeping statement ever? It's like saying cars are not very good - or the sky is not very good!

roger

yea i need this to work

vbx

would like to know if is possible to create the popup alter when the movie is previewed inside a standalone QuickTime player.

Andre

vbx i am interesting that too.. popup on preview movie its very interesting..

student0911

Whenever I read about how QuickTime makes cyberspace more scary or dangerous (JS is JS; I have JS enabled in my browser, but I won't use IE outside the LAN; I just wish I could tell my browser to not load scripts from 3rd-party servers), it reminds me that the most dangerous thing about QuickTime movies is that the site with the most best hijacker-exculpatory 9/11 video evidence, 911blimp.net, chose to use QT (because, like a VCR, it lets the viewer pause and go frame-by-frame in either direction using the keyboard arrow keys) to present its videos. So, to the extent that people can be made to be extra reluctant to even open a .mov file, that helps keep the evidence (and danger to the actual perpetrators) as well-suppressed as it's been. BTW, that site (like this one) uses JS, harmlessly, but its QT videos do not contain any embedded code or scripts of any kind.