# The Analogy of Pop Ups

Art of Third Party POP Up Attacks | Downloading JINX


---

Aditya K Sood
Handle : Zeroknock
http://www.secniche.org

# Abstract

**Art of Third Party Pop up Attacks : Section 1**

This section deals with the latest third party popup attacks that are performed by an attacker from the rogue and vulnerable links of the web sites to circumvent the normal functioning on the web. The target website always seems to be the liable web provider from where the popup attacks are possible. This is the output of my penetration sessions on the web. I have not found any well crafted information regarding these attacks. I will sum up by designing a working algorithm in this aspect and proof of concept how these attacks are done by POPUP manipulators.

**Downloading JINX Through Pop up : Section 2**

This section is based on a very generic problem that occurs while downloading from a website when a popup is initiated from the downloading link. This is a very basic problem now a days because the downloading link is hidden. When the browser is subjugated with the required URL, no downloading occurs or the server displays the HTML web page links but not the downloading link. This is not a core technical layout but can be used as trick for web penetration. I will be very specific in this regard. I find users having lots of problems regarding this so I thought it requires a talk. So there it is.

# Art of Third Party Popup Attacks

**Section 1**

# Concept

You have seen now a days the unnecessary traffic on the web that really disrupts the functioning of the web. This includes the disruptive elements like popups , false linking , redirection elements and poor coded web modules that lead to injection attacks .This specific concept deals with popup attacks that are generated from the third party and from the net that is surmounted to the destination attack point. As the name suggests clearly, the attack base is popup generation but the real concept is how to find the third party with vulnerable link on the web and further relate it or fuse it with the popup elements to get the work done i.e. to lay the attack .Most of the POPUP generation is based on the Javascript tag elements by which some arguments are provided and the popup is generated. This is the specific base of the popup layout. The point here is how this attack is different from the other basic attacks. This attack uses the third party web flaws to lay down popup attack meeting the defined requirements. This is based on hit and trial searching of the desired malfunctioning links on the web which can be used as a base of an attack. I am going to lay down the basic structures first:

**The very basic POPUP generation module :**

```
function PopUp()
{
Netscape = "Netscape.html";
Explorer = "Attack.html";
Unknown = "Unknown.html";
windowprops = "top=0,left=0,resizable=yes" +
",width=" + screen.width + ",height=" + screen.height;
ns = (navigator.appName == 'Netscape');
ie = (navigator.appName == 'Microsoft Internet Explorer');
url = (!ns & !ie) ? unknown : ( ns ? Netscape : Explorer);
window.open(url, "popupPage", windowprops);
}
```

This function in itself is the Popup generator of the parent page .This provides us with the popup properties and kind of popup being generated. This is a kind of primary level generation of popup on the local machines. Now we have undertaken the basic functioning how the popups are generated and put into normal routine to get the work done. The second point is that two requirements should be considered while traversing these types of attacks is that there must be cookie and Javascript enabled on the browser, The attacker can easily be tricked by setting a check status function against the browser which throws the necessary information and the Javascript and cookie status. But now a days Javascript blockers are on the way , but remember human malfeasance has always been there , which is the prime point of exploitation. This is the basic realm which has to be bypassed. That target hit is always more than you expect. The popups are to be generated through Javascript tags so its basic requirement is to set Javascript enabled on the browsers and also cookies. A very basic Javascript routine which checks the browser status and Javascript and cookie check to understand the attack concept

**Routine:**

```
function Javascript_Version()
{
var Is_js;
if (Is_nav2 || Is_ie3) Is_js = 1.0;
else if (Is_nav3) Is_js = 1.1;
else if (Is_opera5up) Is_js = 1.3;
else if (Is_opera) Is_js = 1.1;
else if ((Is_nav4 && (Is_minor <= 4.05)) || Is_ie4) Is_js = 1.2;
```

```
else if ((Is_nav4 && (Is_minor > 4.05)) || Is_ie5) Is_js = 1.3;
else if (Is_hotjava3up) Is_js = 1.4;
else if (Is_nav6 || Is_gecko) Is_js = 1.5;
// NOTE: In the future, update thIs code when newer versions of JS
// are released. For now, I try to provide some upward compatibility
// so that future versions of Nav and IE will show they are at
// *least* JS 1.x capable. Always check for JS version compatibility
// with > or >=.
else if (Is_nav6up) Is_js = 1.5;
// NOTE: ie5up on mac Is 1.4
else if (Is_ie5up) Is_js = 1.3
// HACK: no idea for other browsers; always check for JS version with > or >=
else Is_js = 0.0;
}
function CJCheck()
{
var txtCookie;
var txtJava;
if(window.navigator.cookieEnabled )
{
txtCookie="Test : Window.navigator.cookieEnabled" + "\n" +
"Result : Cookie Enabled On The Browser.";
}
else
{
txtCookie="Test:window.navigator.cookieEnabled\n
Result : Cookie Not Enabled On The Browser.\n";
}
if(window.navigator.javaEnabled() )
{
txtJava = "Test : Window.navigator.JavaEnable" + "\n" +
"Result : Java Enabled On The Browser." + "\n" +
"Cookie : " + document.cookie + "\n" +
"Referrer : " + document.referrer + "\n" +
"Title : " + document.title + "\n" +
"LastMod : " + document.lastModified + "\n"
"HIstory Length : " + hIstory.length + "\n" +
"Screen Width : " + screen.width + "\n" +
"Screen Height : " + screen.height;
}else{
txtJava="Test: window.navigator.JavaEnabled \n
Result : Java Not Enabled On The Browser.";}
txtOutput.value=txtCookie + "\n" + txtJava;
}
```

The two modules are clearly defined the Javascript version check and Javascript enabled/disabled status of the web browser , now the base is already being set , we are going to understand the algorithm to meet the attack requirements

**The Third Party Popup Attack Layout**

A] First Of all an attacker crawls through the web to find the vulnerable links in major service providers like MSN, Amazon , AOL , Yahoo , Gmail , Google etc. The point here is that the vulnerable point serves as an attack base for launching on the fly attack to the third party. In this

an attacker always considers that rogue link should be exploited through Javascript i.e. inclusion of Javascript tags, injections and mainly the popup can be generated through that rogue link.

B] Secondly, that search has to be made in a crafty manner i.e. its not so easy to find vulnerable links with a specification of your kind. The way an attacker creates it basically depends on the capability of hacker and how he gets the work done. My point is to find the links that suits the attack can be eased through Google search engine. The search should work like this:

**Google Hacking:**

*inurl:asmx site:amazon.com*
*allinurl:jws site:ebay.com*
*inurl:redirect.php site:msn.com*

These are the crafty requests that leverage a lot of information. But my point is always to find the server error,htm or servererro.asp or servererro.aspx page or any page having error stats in it. This is my priority because the code is rather more vigorous in exploitation because of inclusion of server stats in it. It depends on the thinking and problem handling capability of an attacker to find the vulnerable link of its specific kind.

*inurl:error.html site:aol.com*
*inurl:servererror.html site:msn.com*

The hit and trial works very well in this.

C] Thirdly, you can also find the vulnerability through redirection links because a lot of popup enabled stuff can be seen on the web. There you have to judge whether the exploitation can be done or not. It's also necessary to go after redirection pages and understand the code these pages are using to redirect to the destination.

D] After lot of enumeration you find a number of links but our main point is that :

D.1] After injecting Javascript in the URL, the popup must originate to serve as the third party attack base, either this should be found directly or one should undertake crafty techniques

D.2] The popup origin should be done after the exploitation of the link. This must initiate the popup from the server that is from any service provider (AOL Amazon etc) whose URL link is being exploited. This exploited popup generation is very crucial for the defined attack.

E] There should be a proper execution check performed to set the base correctly. This is done to ensure that there is proper handling of attack base to lay an attack.

F] Now the time is to craft a defined code for fly hacking. A very definitive Javascript code is written which sets a link correlation with the attack base.

The Fly-Attack through the Email is performed. The strategy works in this way.

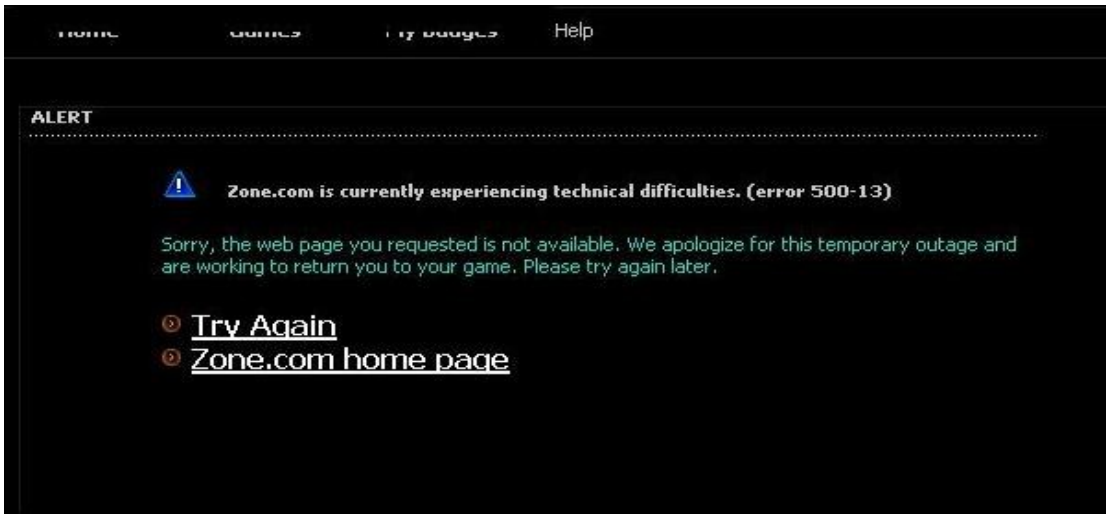
**Practical Proof Of Concept:**

Here I am providing you a practical proof of concept of this third party pop Attack. My attack point goes with search on google. I am not going to enlist the provider with various searches that I have done while undertaking this rogue request, just going to enlist steps with snapshots.

**Finding vulnerable link**

*inurl:servererror.htm site:<service provider>*
*inurl:asmx site:<service provider>*

The Rogue Link I found is :




After injecting Javascript attack I found that popup is generated through it. With a designed lopp script the Pop can be called again and again .The required snapshot is encapsulated as:


As this clearly shows that our exploited link generates popup from that service provider. So this serves as the third party attack base i.e. the URL with exploitable parameters. We have to find that site which generates pop ups and is deteriment to our attack scenario

Remember two points , in designing code.

A] The code should be with time limits i.e. it executes at specific time.
B] Without time limits, the system will get in bedazzled state.

It depends all in all on hacker's viewpoint.

**Inference:**

The web is attack prone. There are new parameters driving various type of attacks, but they serves as a knowledge pool to understand the hidden elements of web. Rest the penetration goes on.

# Popup Downloading JINX

**Section 2**

# Explanation

You get to some specific website and you are in a need to download the material from that website. You get to that link but a popup is generated rather than download , even after the popup the google adds or other advertising material are displayed. You try one or two times but the phenomenon goes in the same direction. What actually the problem is that the link does not allows you to download the stuff. This kind of problem occurs with the servers or websites that hold the material which is very genuine and rare to find. The resources are there on the web server itself but the links are so craftily carved that results in no direct download and really frustrating the users. The resources can also be locked down on the server to hinder unauthorized access. This is also done to enhance security and minimize illegal transactions.

There are three specific downloading stats of websites:
A] There is direct download as soon as you click on the link.
B] There is no direct download but you require password to unlock resource.
C] There is a download and the link holds the pass but is hidden.

These three cases are considered as generic layouts of website downloading. These can be fused with popups generation to link to the third party or advertising when ever an unauthorized request for downloading comes to the server. When ever server finds these types of requests, the underlined responses are generated:

A] The link is forbidden.
B] The resource is not found on this server.
C] Linking to third party Popups.
D] Direct unauthorized access.

Our point of main discussion is what happens whenever a popup is generated from the pressed link and how to bypass that with the trick to download the resource. You can also play a direct trick here on the server and use the link undertaken in the browser to trace the index of files, this works in many cases but not all.

**Practical Example:**
Lets say there is a link:

***http://www.tomcfa.com/download/cfa/2006-07-***
*16/5e0846262d23757f2ce4651dd3ea5514.html#edown*

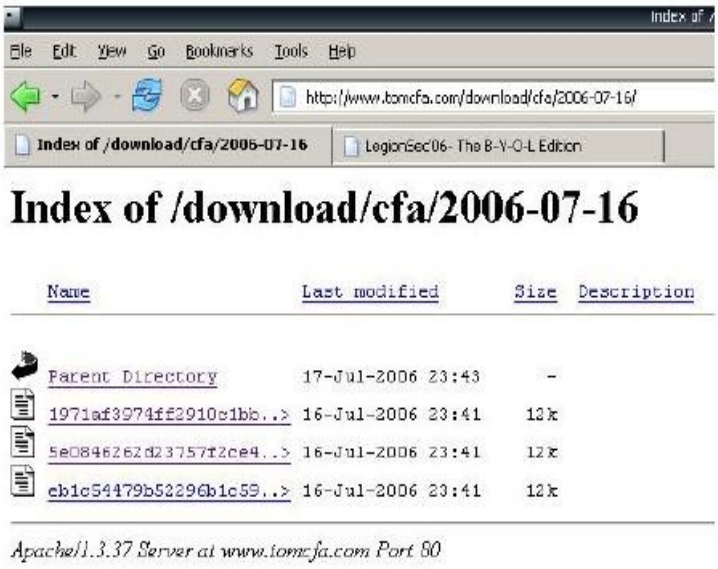
This link when re-open again and again, it is being redirected to the same pages. So a better trick is to look into its index by two ways

A] By Google Query of inurl:index of
B] Directly if possible.

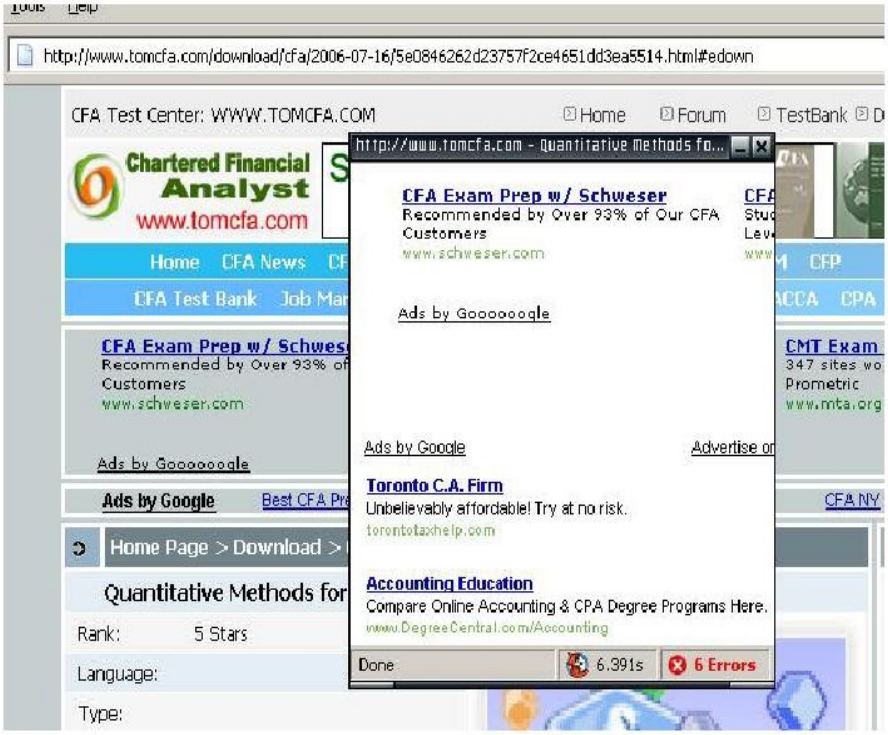
**Exemplary Layout :**

http://www.tomcfa.com/download/cfa/2006-07-16/

The URL has been dissected , now look at the response we have:



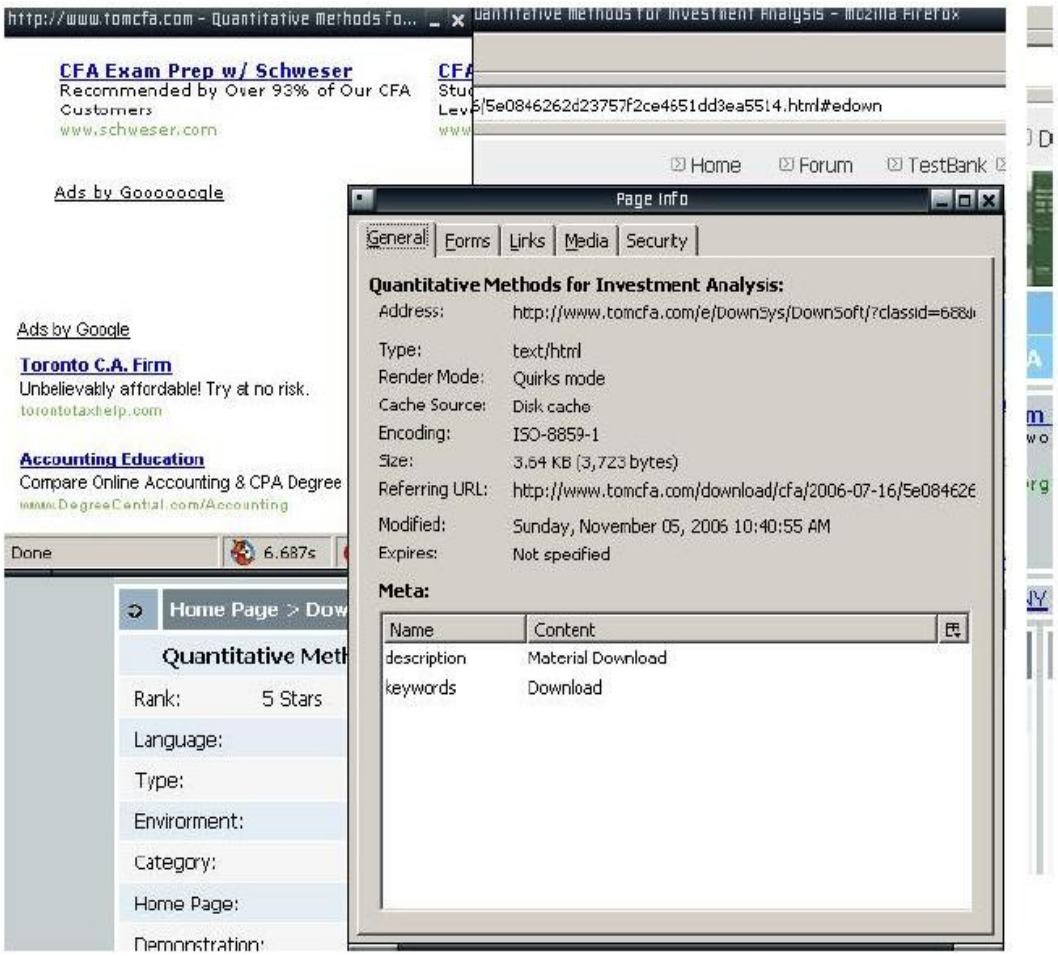

In this case the direct traversal of the directory link is possible from the URL by stripping down the parameters but it is not dependable. Moreover, it indexes only html pages and provides no links to the download materials or required resources. Now I get back again to the desired web page and look into the downloading link from where the popup initiates. Let's see after clicking downloading the link what I got:




As we can see very clearly after clicking the downloading link, a popup is initiated but if seen in a

clear context it is just advertising the website. So where the actual downloading link is? .It must be hidden somewhere, that's where the anatomy of a popup lies. This process is repeated several times but of no use. Then of course a trick is undertaken. We will analyze the popup in all respects to extract maximum information. Let's begin with it.

When I looked into page info I have got this:




If you look you will find that in Meta Specification, the description tag and the keyword tag directly leverage the fact that this popup does have downloading information. It is hidden somewhere and one can very clearly extract the general information regarding the popup. A lot of information can be carved from the property page with detailed analysis. But our point of concern is to find the links that are holding the information. The next point is to also find the links related to this popup. I initiated a click on the links tab and see what I have undertaken.

.

General | Forms | Links | Media | Security

| Name | Address | Type |
|---|---|---|
| CFA Exam Prep w/ Schweser | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=B59p4F4BNRaWQJKGUhQOQieyeDvfk2xznqLq... | Anchor |
| CFA Exam Course | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BXExiF4BNRaWQJKGUhQOQieyeDr-92BnJhLuN... | Anchor |
| <!-- nw='#000000';nw=nw.sli... | http://services.google.com/feedback/abg?ur=http://www.tomcfa.com/e/DownSys/DownSoft/%3Fclassid%... | Anchor |
| Advertise on this site | https://adwords.google.com/select/OnsiteSignupLandingPage?client=ca-pub-0632677162515737&referring... | Anchor |
| Toronto C.A. Firm | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BfnFSG4BNRf7_HJ2ihAP45vXpDuOznRy51crG... | Anchor |
| Accounting Education | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BWjAeG4BNRf7_HJ2ihAP45vXpDuvX9QzDsY2f... | Anchor |
| CMT Exam Now Computerized | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BTmdwG4BNRf7_HJ2ihAP45vXpDpes2wjN0ayB... | Anchor |
| <!-- nw='#000000';nw=nw.sli... | http://services.google.com/feedback/abg?ur=http://www.tomcfa.com/e/DownSys/DownSoft/%3Fclassid%... | Anchor |
| Advertise on this site | https://adwords.google.com/select/OnsiteSignupLandingPage?client=ca-pub-0632677162515737&referring... | Anchor |
| CMA Exam Preparation | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BAp9fGIBNRY6mH6e2hAOOqbD8DvD99haMu9... | Anchor |
| Financial Reporting Help | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BhcgzGIBNRY6mH6e2hAOOqbD8Dom0lh_dqY2... | Anchor |
| | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&num=0&client=ca-ref-pub-0632677162515737&a... | Anchor |
| stylesheet | http://www.tomcfa.com/e/data/images/css.css | Stylesheet |
| | http://www.tomcfa.com/e/enews?enews=DownSoft&classid=68&id=20&pathid=0&pass=c8a749b8427bcc... | Anchor |
| CFA ® Financial Analyst | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BhESMF4BNRaWQJKGUhQOQieyeDu23oBe13e... | Anchor |
| <!-- nw='#000000';nw=nw.sli... | http://services.google.com/feedback/abg?ur=http://www.tomcfa.com/e/DownSys/DownSoft/%3Fclassid%... | Anchor |
| Advertise on this site | https://adwords.google.com/select/OnsiteSignupLandingPage?client=ca-pub-0632677162515737&referring... | Anchor |
| PASSPRO for FRM | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BcF0uG4BNRf7_HJ2ihAP45vXpDsqYQs7qyQHA... | Anchor |

Now I have got a number of links. If you look at this, there is a one link of tomcfa with no name specification as:

General | Forms | Links | Media | Security

| Name | Address | Type |
|---|---|---|
| CFA Exam Prep w/ Schweser | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=B59p4F4BNRaWQJKGUhQOQieyeDvfk2xznqLq... | Anchor |
| CFA Exam Course | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BXExiF4BNRaWQJKGUhQOQieyeDr-92BnJhLuN... | Anchor |
| <!-- nw='#000000';nw=nw.sli... | http://services.google.com/feedback/abg?url=http://www.tomcfa.com/e/DownSys/DownSoft/%3Fclassid%... | Anchor |
| Advertise on this site | https://adwords.google.com/select/OnsiteSignupLandingPage?client=ca-pub-0632677162515737&referring... | Anchor |
| Toronto C.A. Firm | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BfnFSG4BNRf7_HJ2ihAP45vXpDuOznRy51crG... | Anchor |
| Accounting Education | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BWjAeG4BNRf7_HJ2ihAP45vXpDuvX9QzDsY2f... | Anchor |
| CMT Exam Now Computerized | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BTmdwG4BNRf7_HJ2ihAP45vXpDpes2wjN0ayB... | Anchor |
| <!-- nw='#000000';nw=nw.sli... | http://services.google.com/feedback/abg?url=http://www.tomcfa.com/e/DownSys/DownSoft/%3Fclassid%... | Anchor |
| Advertise on this site | https://adwords.google.com/select/OnsiteSignupLandingPage?client=ca-pub-0632677162515737&referring... | Anchor |
| CMA Exam Preparation | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BAp9fGIBNRY6mH6e2hAOOqbD8DvD99haMu9... | Anchor |
| Financial Reporting Help | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BhcgzGIBNRY6mH6e2hAOOqbD8Dom0lh_dqY2... | Anchor |
| | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&num=0&client=ca-ref-pub-0632677162515737&a... | Anchor |
| stylesheet | http://www.tomcfa.com/e/data/images/css.css | Stylesheet |
| | http://www.tomcfa.com/e/enews?enews=DownSoft&classid=68&id=20&pathid=0&pass=c8a749b8427bcc... | Anchor |
| CFA ® Financial Analyst | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BhESMF4BNRaWQJKGUhQOQieyeDu23oBe13e... | Anchor |
| <!-- nw='#000000';nw=nw.sli... | http://services.google.com/feedback/abg?url=http://www.tomcfa.com/e/DownSys/DownSoft/%3Fclassid%... | Anchor |
| Advertise on this site | https://adwords.google.com/select/OnsiteSignupLandingPage?client=ca-pub-0632677162515737&referring... | Anchor |
| PASSPRO for FRM | http://pagead2.googlesyndication.com/pagead/iclk?sa=l&ai=BcF0uG4BNRf7_HJ2ihAP45vXpDsqYQs7qyQHA... | Anchor |

This link looks something different from rest of links when looking at its parameters, I found:

*http://www.tomcfa.com/enewsenews=DownSoft&classid=68&id=20&pathid=0&pass=c8a749b8427bcc9a01d3e9f53e0a887a&p=:::*

Now I found the : Path ID and pass and this makes me sure that this is the download link. I test it by copying it into browser address bar and as rightly expected the downloading starts. The trick really works in most of the cases. It works and works very well .

**Inference**

The pop up jinx of downloading is there but the web is a knowledge pool. we just need to integrate it. The knowledge and the information lies there waiting to be traced.