# Windows 7 Security Test

Windows 7 vs The Malware-Injecting Web Site
It's Go Time

# Background

A friend's computer was infected when she received a link on her Facebook account from another friend, also on Facebook. That link went to a web site which created a pop up window. The pop up stated her computer was "infected" and provided a program to remove the infection. Unknowingly, she ran the program, which proceeded to infect her computer. It required the services of a professional service to return her computer to working condition.

However, in the meantime, her Facebook account proceeded to post strange links on her "wall". That's the basis of this report.

The purpose of this test is to determine how easily a suspected malware-injecting web site can infect a Windows 7 system. One of these links will be entered into the address bar of Internet Explorer 8.0 running on Windows 7, using the protocol listed on page 4.

# WARNING NOTICE

The original web sites used for this experiment are most likely still active and can infect the system of someone who does not take the requisite precautions (as has been done with running this experiment). Therefore, if you're not certain of what you're doing, DO NOT VISIT THE SITES LISTED IN THIS REPORT!

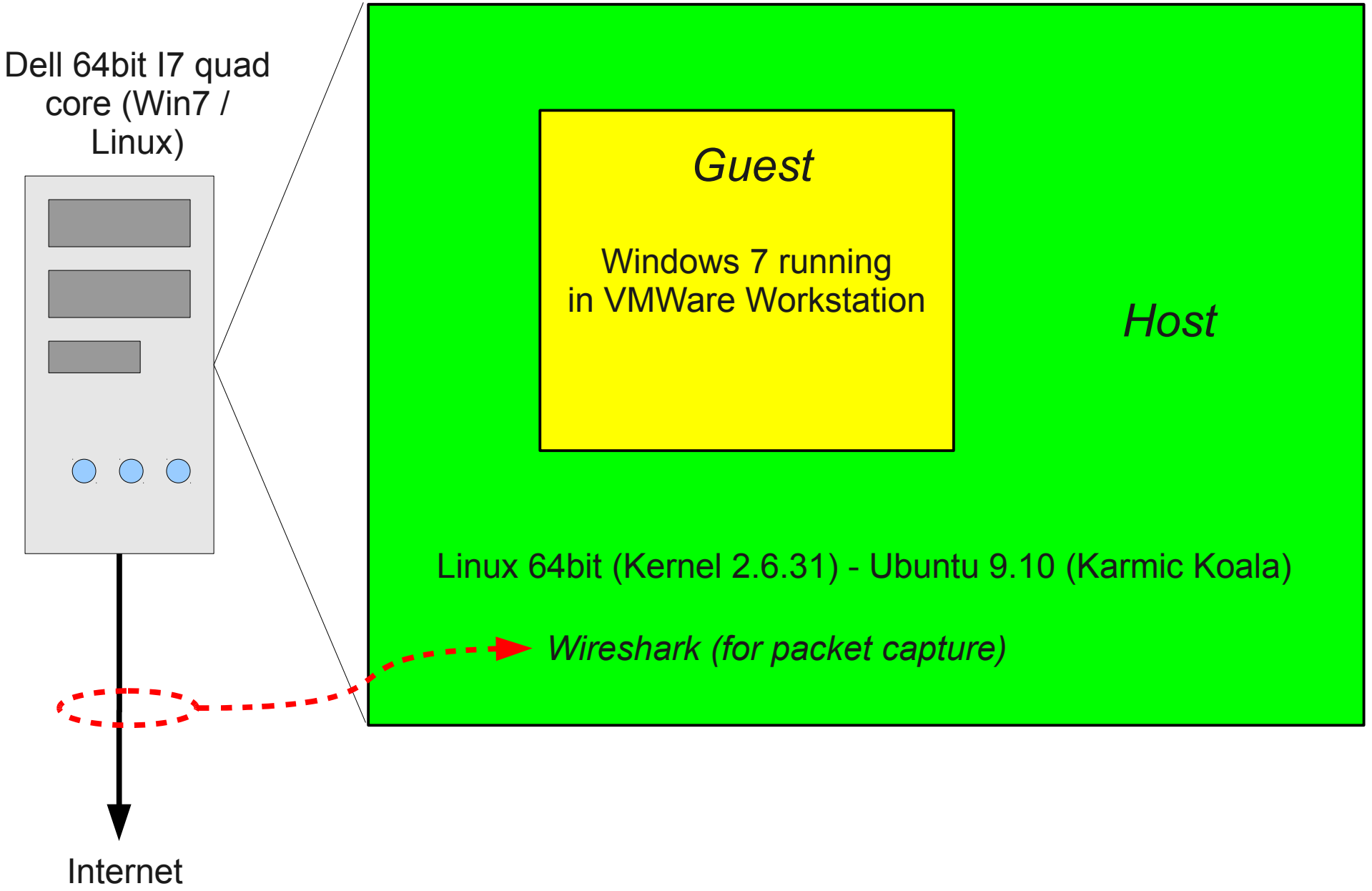
You've been warned.

# Test Protocol

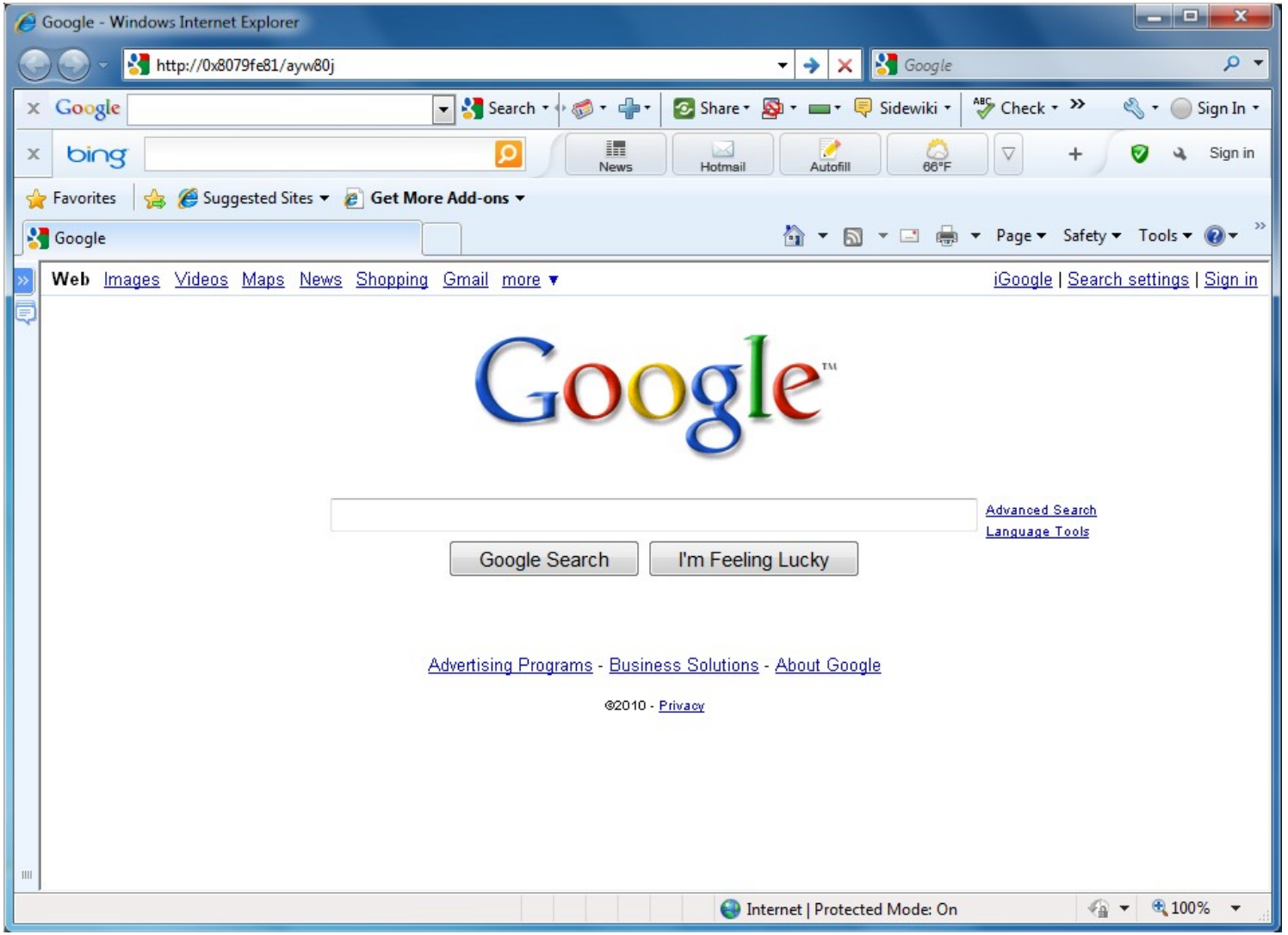
The protocol for this was as follows:

• Run a virtual machine (using VMWare Workstation) running Windows 7 Professional as the operating system.
• Ensure that the operating system has all of the latest updates, according to the "Update" feature in Windows "Control Panel".
• Use Internet Explorer 8.0 for web access.
• Operate everything with the defaults, such as a person without any special technical knowledge would most likely do.
• Use an antivirus program. In this case, the program was Kaspersky Internet Security Suite 2010. Again, it also had the latest updates and virus signatures.
• All web pages would be accessed using a "limited" account, not the "administrator" account with which Windows starts.
• Create 10+ digit passwords for both the administrator and limited accounts. The passwords consisted of random strings of upper and lowercase alphabetic characters, numbers (0 - 9), and special characters (@, $, #, %, &, etc).
• **If a website provided a pop up window of any kind stating, "Run" or "Okay", it would be clicked.**
• Capture all internet traffic using Wireshark.

# System Set-up



# The Beginning




To start, the URL was entered directly into the Internet Explorer address bar. After that, it was "off to the races".

Initial URL (http://0x8079fe81/ayw80j) ← **Start by entering this URL into the Internet Explorer address bar...**

IE to server: Hey, do you have the file *ayw80j*?

Server response: Nope, go here and ask for file *95362* in the directory *yourdvd.*

http://portalecomuni.it/

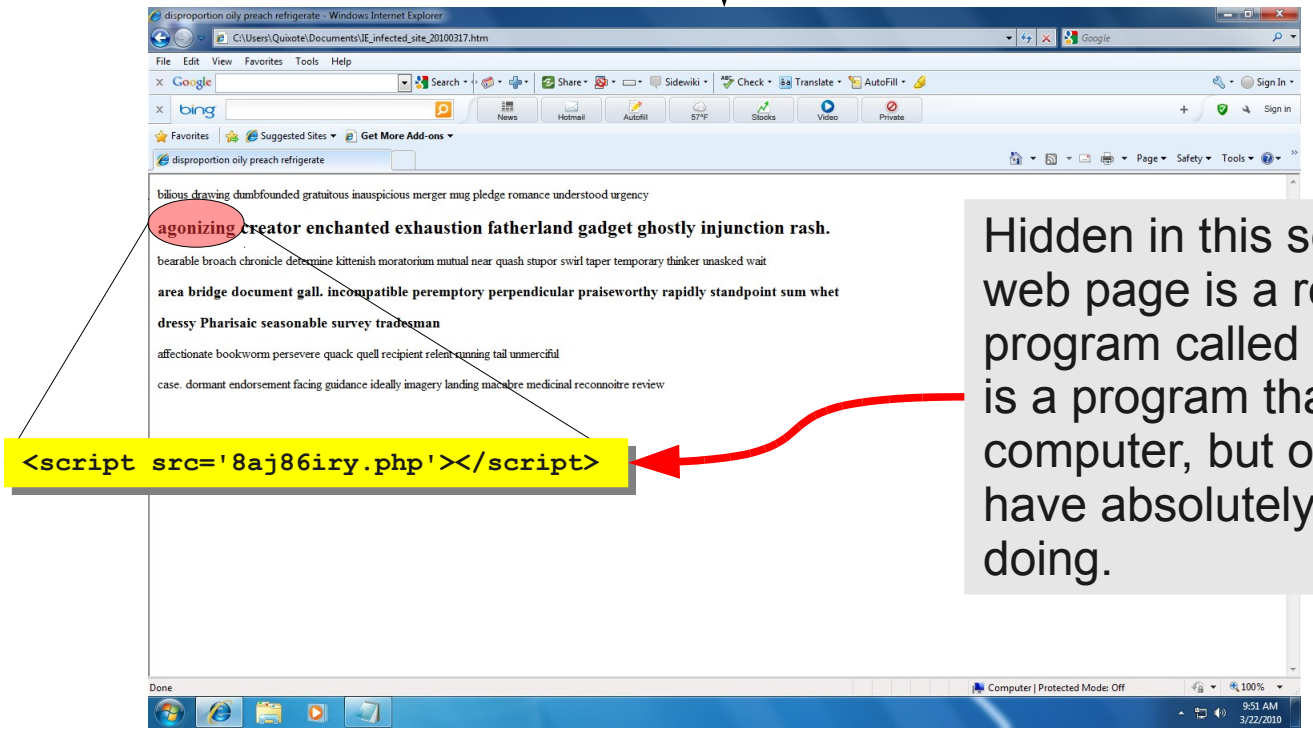
IE: Do you have the file 95362?

Server: Nope, go here and ask.

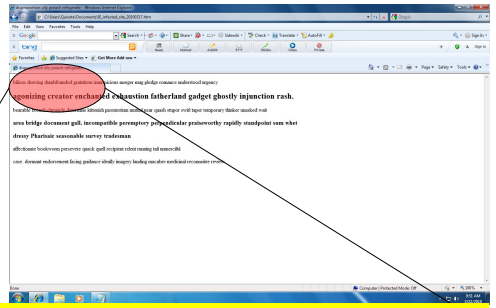
http://www.portalecomuni.it/

IE: Do you have the file 95362?

Server: Why, yes, I do. Here ya go! (rubs hands and laughs evilly...and loads a web page that appears to consist of nothing more than random words in different size fonts)




Hidden in this seemingly innocuous web page is a request to run a program called "8aj86iry.php". This is a program that will not run on your computer, but on the server, so you have absolutely no idea what it is doing.



```
<script src='8aj86iry.php'></script>
```

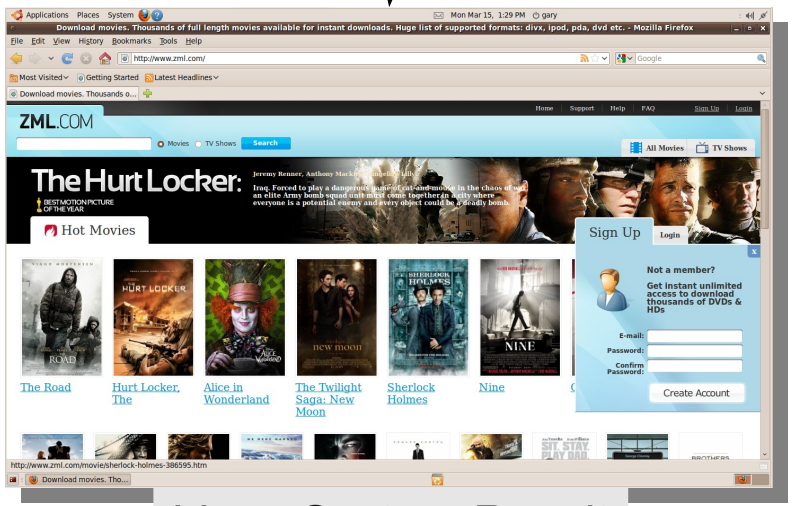
Call: Run 8aj86iry.php

Response for a Windows-based system: Here is some Javascript code that I want you to run.

```
var a6657 = [
["fqiadhceigblhojdodjkg.chhirom".replace(/[qidhgljr]+/g,""),'fb2'],
["tangbngirlehrdi.rcnlolmnb".replace(/[nbirlh]+/g,""),'tg'],
["fkrjblienbdhjsbgtljeahrj.gcbgomkk".replace(/[kjblhga]+/g,""),'fr'],
["mjbjhynjbsrilprbidraiclneg.grcqbqolbfjmk".replace(/[jbhnrildgqfk]+/g,""),'ms'],
["mfhsdfpqeljgiebnkhfs.ecjjodhme".replace(/[fhdqejgb]+/g,""),'ms'],
["ltneickoeu.irpombpsofbu".replace(/[teicourpbf]+/g,""),'ms'],
["mfyjlyilefagprddjbojnhofkip.piplcnomhl".replace(/[fjligpdnh]+/g,""),'yb'],
["fgugeehqbeehakrll.lncenojqmd".replace(/[gehqklnjd]+/g,""),'fu'],
["tpwpihnpttgenlrjf.djcfgjqodnhmhakb".replace(/[phngljfdqakb]+/g,""),'tw'],
["hdqkien5kd.nackbojslmeup".replace(/[dqkenabjslup]+/g,""),'hi5'],
["bgkqeqjbfuhnuoqljrh.kjaicgokumkah".replace(/[gkqjfuhnlrai]+/g,""),'be']
];
var b41bca = [
'94.16' + '9.6.105',
'77.78.' + '169.72',
'201.2' + '20.78.171',
'81' + '.57.237.246',
'65.32' + '.70.169',
'68' + '.146.40.37',
'6' + '8.80.92.193',
'89.1' + '76.106.238',
'82' + '.13.162.180',
'75.' + '228.54.56',
'84.22' + '0.234.190',
'69.201' + '.132.169',
'65.3' + '2.181.175',
'201.1' + '64.107.134',
'82' + '.228.220.165',
'65' + '.33.118.48',
'62.' + '72.251.182',
'99.234' + '.232.6',
'7' + '9.107.30.47',
'68.' + '62.21.71',
''];
... (a lot more code snipped)...
```

Windows System Result

Response for a Linux-based system: I'm not even going to bother with you. Just go to the website http://www.zml.com.

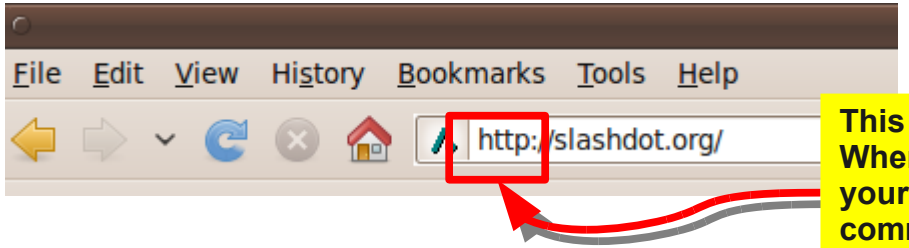



Linux System Result

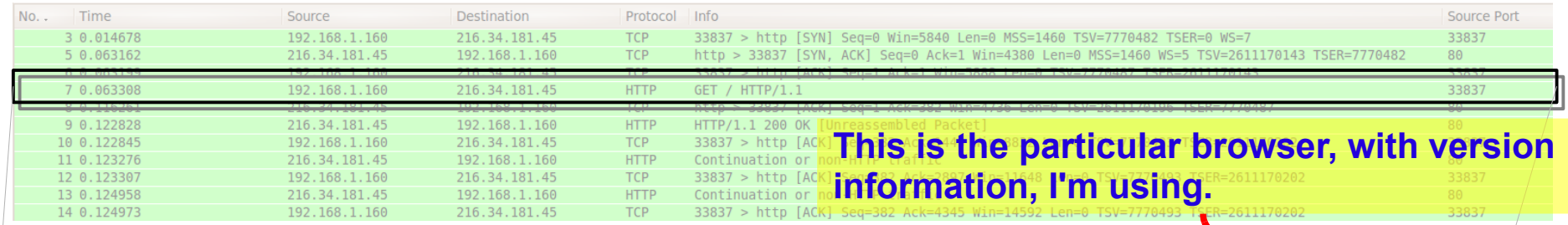
# *Sidenote: How Does The Internet Know My Computer & Browser?*

Short Answer: You tell it.

Long Answer: When you open your browser and go to a particular web page, you're using the hypertext transfer protocol or "HTTP". (Ever wonder why the browser always says, "http://..."?)




**This means that the browser is using the hypertext transfer protocol. When you enter the URL (*http://slashdot.org*, in this case) and hit "Enter", your browser connects to the server (more on that later) and sends a command called "GET". As part of that command, your browser sends a string, called a token, that starts with "User-Agent", as shown below.**




**This is the particular browser, with version information, I'm using.**

**User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.8) Gecko/20100214 Ubuntu/9.10 (karmic) Firefox/3.5.8**

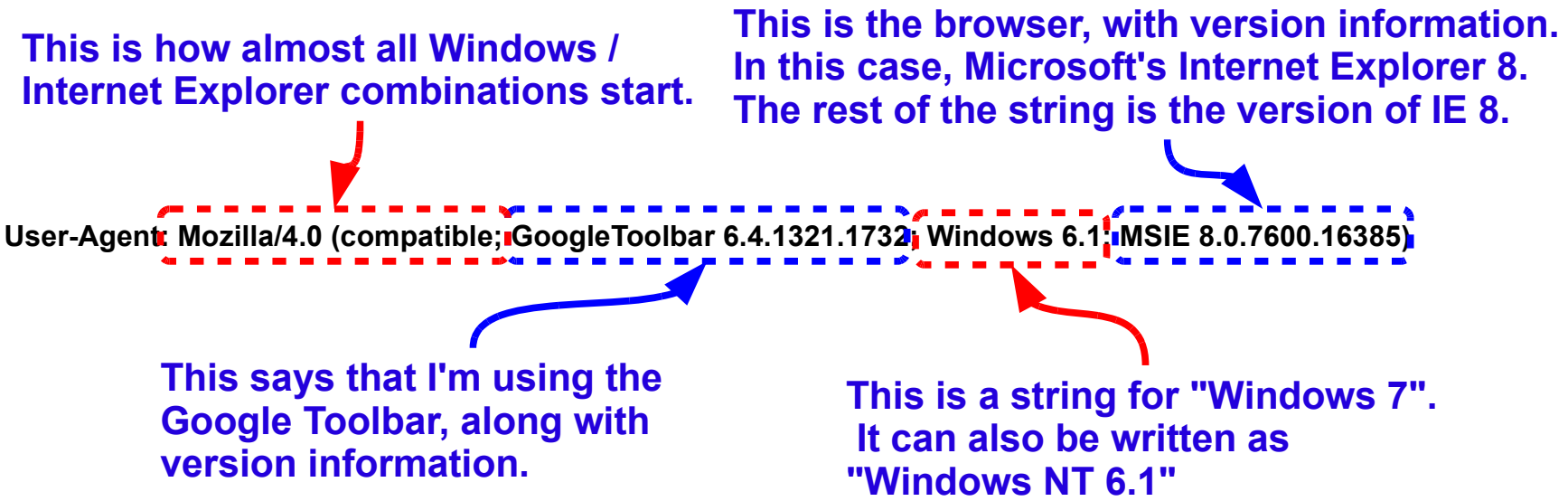
**This provides information on my computer; in this case, my computer is a 64-bit ("_64") Intel-based ("x86") running Linux.**

**This provides information on my operating system, which in this case is Ubuntu version 9.10. This version has the name of "Karmic Koala".**

**This information is supposed to be used to ensure that the server provides content that your browser can properly display. However, criminals use this information to properly target (or NOT target) your system.**

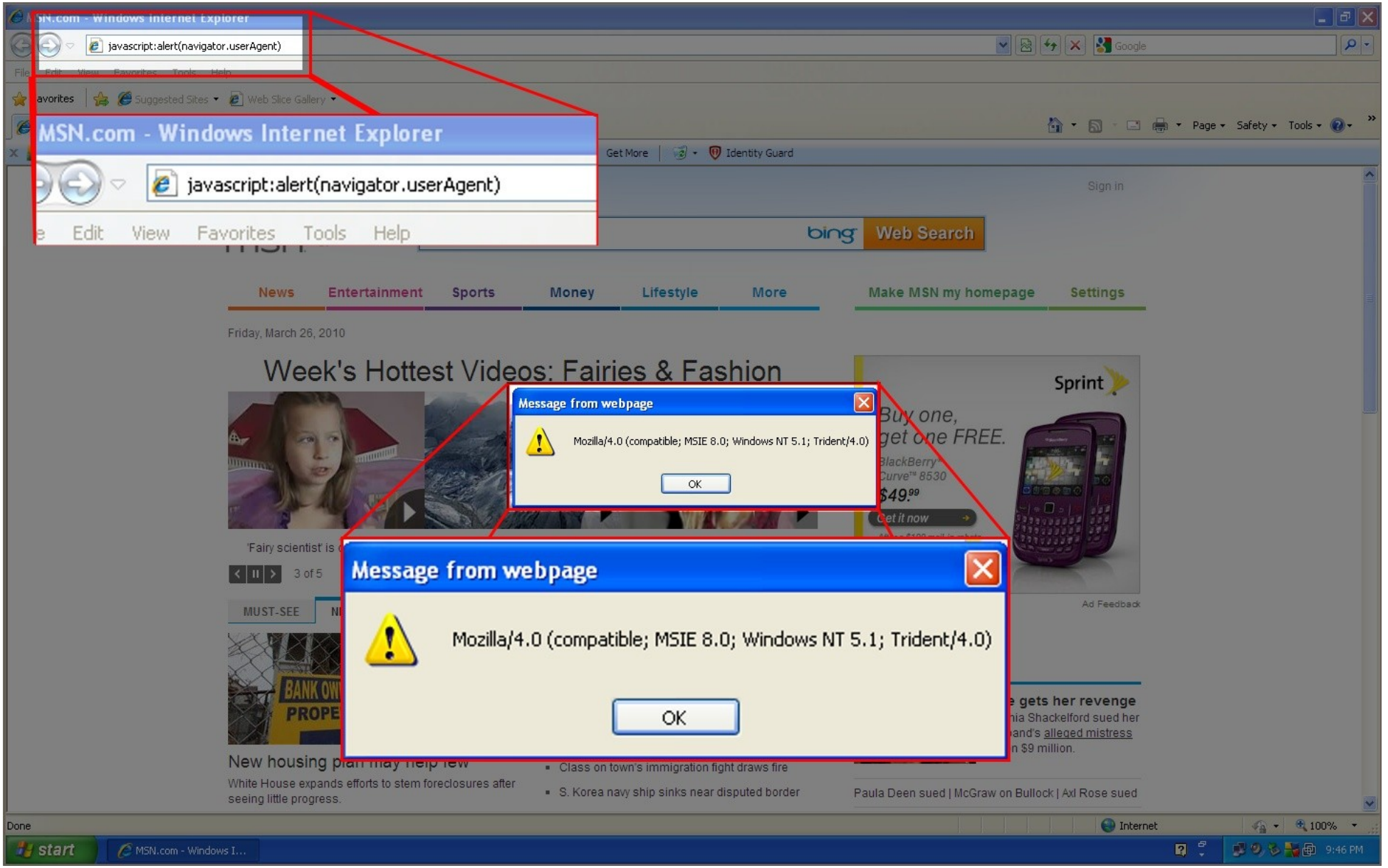
# *Sidenote: How Does The Internet Know My Computer & Browser?*

Another example of the User-Agent information string is:



If you want to know what your User-Agent string says when you request a web page, type this in your address bar:

***javascript:alert(navigator.userAgent)***



Where were we? Oh, yeah. If you're running Windows, the server will send you a bunch of obfuscated Javascript. The general purpose of the Javascript is (1) to determine which (if any) social network website you came from and (2) to connect you with at least one other computer that will download the actual malicious code.

```
var a6657 = [
["fqiadhceigblhojdodjkg.chhirom".replace(/[qidhgljr]+/g,""),'fb2'],
["tangbngirlehrdi.rcnlolmnb".replace(/[nbirlh]+/g,""),'tg'],
["fkrjblienbdhjsbgtljeahrj.gcbgomkk".replace(/[kjblhga]+/g,""),'fr'],
["mjbjhynjbsrilprbidraiclneg.grcqbqolbfjmk".replace(/[jbhnrildgqfk]+/g,""),'ms'],
["mfhsdfpqeljgiebnkhfs.ecjjodhme".replace(/[fhdqejgb]+/g,""),'ms'],
["ltneickoeu.irpombpsofbu".replace(/[teicourpbf]+/g,""),'ms'],
["mfyjlyilefagprddjbojnhofkip.piplcnomhl".replace(/[fjligpdnh]+/g,""),'yb'],
["fgugeehqbeehakrll.lncenojqmd".replace(/[gehqklnjd]+/g,""),'fu'],
["tpwpihnpttgenlrjf.djcfgjqodnhmhakb".replace(/[phngljfdqakb]+/g,""),'tw'],
["hdqkien5kd.nackbojslmeup".replace(/[dqkenabjslup]+/g,""),'hi5'],
["bgkqeqjbfuhnuoqljrh.kjaicgokumkah".replace(/[gkqjfuhnlrai]+/g,""),'be']
];
var b41bca = [
'94.16' + '9.6.105',
'77.78.' + '169.72',
'201.2' + '20.78.171',
'81' + '.57.237.246',
'65.32' + '.70.169',
'68' + '.146.40.37',
'6' + '8.80.92.193',
'89.1' + '76.106.238',
'82' + '.13.162.180',
'75.' + '228.54.56',
'84.22' + '0.234.190',
'69.201' + '.132.169',
'65.3' + '2.181.175',
'201.1' + '64.107.134',
'82' + '.228.220.165',
'65' + '.33.118.48',
'62.' + '72.251.182',
'99.234' + '.232.6',
'7' + '9.107.30.47',
'68.' + '62.21.71',
''];
... (a lot more code snipped)...
```

This is Javascript code that is obfuscated (real words mixed with random letters) to conceal what it is trying to do. These lines, when the random letters are removed, reveal the URL of all of the major social networking sites. This includes:

- facebook.com
- tagged.com
- friendster.com
- myspace.com
- myyearbook.com

To understand how the code is being purposely-made confusing, you need to understand how it's allowing your system to decode it. The URLs of the social networking sites (facebook, tagged, myspace, etc) are put into a string, then random letters are injected between the letters of the URL. The system then creates a Javascript command that tells your system how to decode it. To you, it looks like computer guacamole. Your computer, however, has no problem understanding it.

```
["fidhajqncqrejbppohojjkhg.rdqcgirohigmhh".replace(/[idhjqnrpg]+/g,""),'fb2'],
["tlaigljgrqerhkdlh.cjojjjmp".replace(/[lijrqhkp]+/g,""),'tg'],
["fhalbrkiaelglnbadsktehhrhk.ckolmlg".replace(/[halbkg]+/g,""),'fr'],
["mynjjbshprbjajicder.kqlciqoidmnkn".replace(/[njbhridkql]+/g,""),'ms'],
["mdsjpliefgndkasgd.acfjoamfa".replace(/[djefga]+/g,""),'ms'],
["lafngotker.tqcmjdspq".replace(/[afgoterqcjdp]+/g,""),'ms'],
["mjyfhlyhneqhqaflridbpohioflkidpj.gcqqojgpmg".replace(/[jfhlnqidpg]+/g,""),'yb'],
["fukbljaljrjp.clhoqmhdp".replace(/[kljphqd]+/g,""),'fu'],
["tdwabbqilgptjpthfehnrlqjb.kpgcqogfpmp".replace(/[dabqlgpjhfnk]+/g,""),'tw'],
["hkpiqt5ffdt.ulckodmsn".replace(/[kpqtfdulsn]+/g,""),'hi5'],
["brkkepkbnhsos.lcpinodiukjmds".replace(/[rkpnhsliduj]+/g,""),'be']
```

**["fidhajqncqrejbppohojjkhg.rdqcgirohigmhh".replace(/[idhjqnrpg]+/g,""),'fb2']**

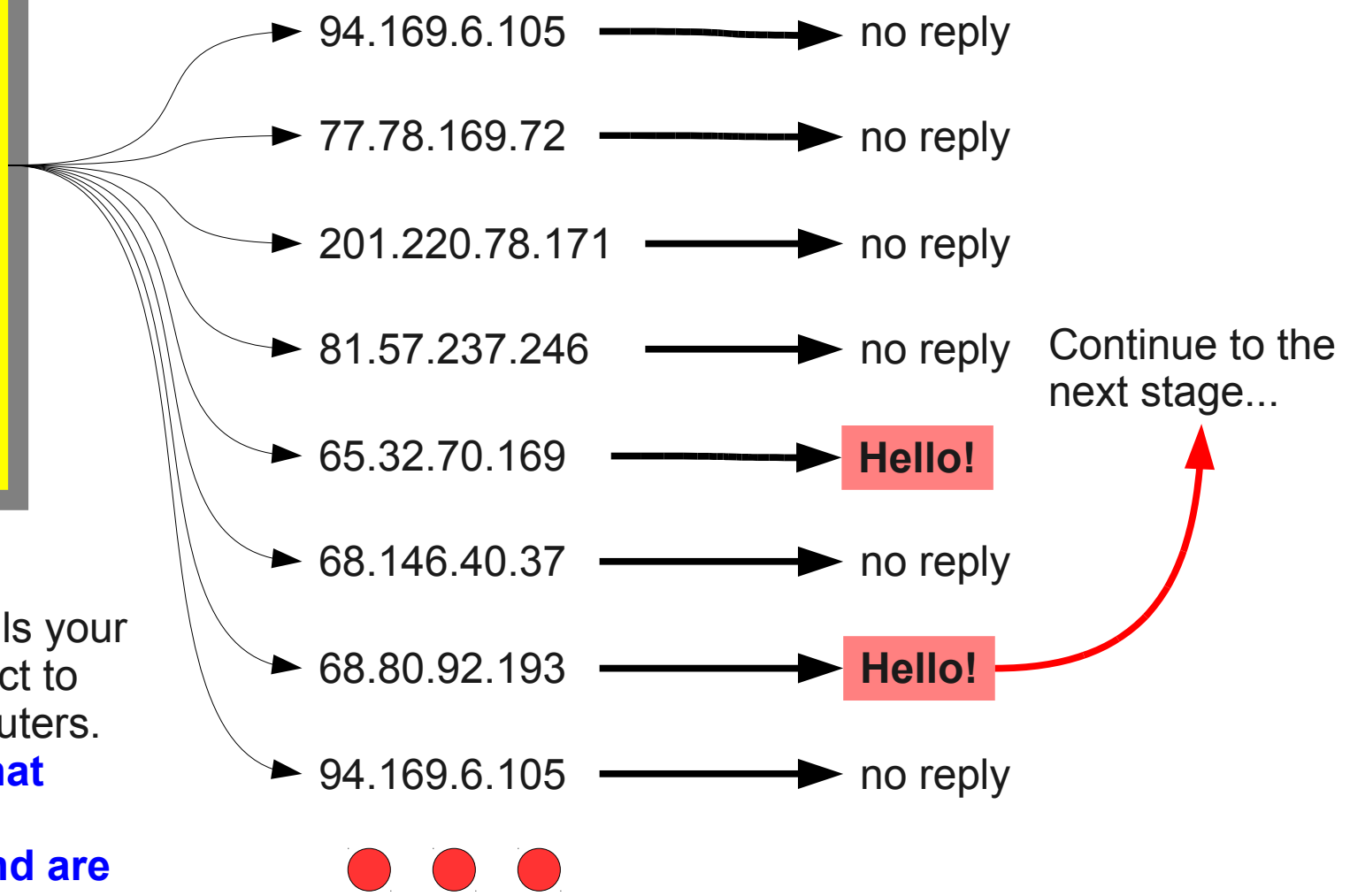
**facebook.com**

This code means to remove the letters between the [ ] brackets, meaning it removes any of the letters **idhjqnrpg,** from the string at left. Once done, the string formed is "facebook.com".

```
var a6657 = [
["fqiadhceigblhojdodjkg.chhirom".replace(/[qidhgljr]+/g,""),'fb2'],
["tangbngirlehrdi.rcnlolmnb".replace(/[nbirlh]+/g,""),'tg'],
["fkrjblienbdhjsbgtljeahrj.gcbgomkk".replace(/[kjblhga]+/g,""),'fr'],
["mjbjhynjbsrilprbidraiclneg.grcqbqolbfjmk".replace(/[jbhnrildgqfk]+/g,""),'ms'],
["mfhsdfpqeljgiebnkhfs.ecjjodhme".replace(/[fhdqejgb]+/g,""),'ms'],
["ltneickoeu.irpombpsofbu".replace(/[teicourpbf]+/g,""),'ms'],
["mfyjlyilefagprddjbojnhofkip.piplcnomhl".replace(/[fjligpdnh]+/g,""),'yb'],
["fgugeehqbeehakrll.lncenojqmd".replace(/[gehqklnjd]+/g,""),'fu'],
["tpwpihnpttgenlrjf.djcfgjqodnhmhakb".replace(/[phngljfdqakb]+/g,""),'tw'],
["hdqkien5kd.nackbojslmeup".replace(/[dqkenabjslup]+/g,""),'hi5'],
["bgkqeqjbfuhnuoqljrh.kjaicgokumkah".replace(/[gkqjfuhnlrai]+/g,""),'be']
];
var b41bca = [
'94.16' + '9.6.105',
'77.78.' + '169.72',
'201.2' + '20.78.171',
'81' + '.57.237.246',
'65.32' + '.70.169',
'68' + '.146.40.37',
'6' + '8.80.92.193',
'89.1' + '76.106.238',
'82' + '.13.162.180',
'75.' + '228.54.56',
'84.22' + '0.234.190',
'69.201' + '.132.169',
'65.3' + '2.181.175',
'201.1' + '64.107.134',
'82' + '.228.220.165',
'65' + '.33.118.48',
'62.' + '72.251.182',
'99.234' + '.232.6',
'7' + '9.107.30.47',
'68.' + '62.21.71',
''];
... (a lot more code snipped)...
```

These are IP addresses, most likely individual's personal computers that have been infected and are now part of a botnet. In all, there are 20 computers listed. Note that, each time you go through this process, it's possible you will get back 20 different computers. The botnet controllers are probably choosing from a (very large) pool of infected personal computers.

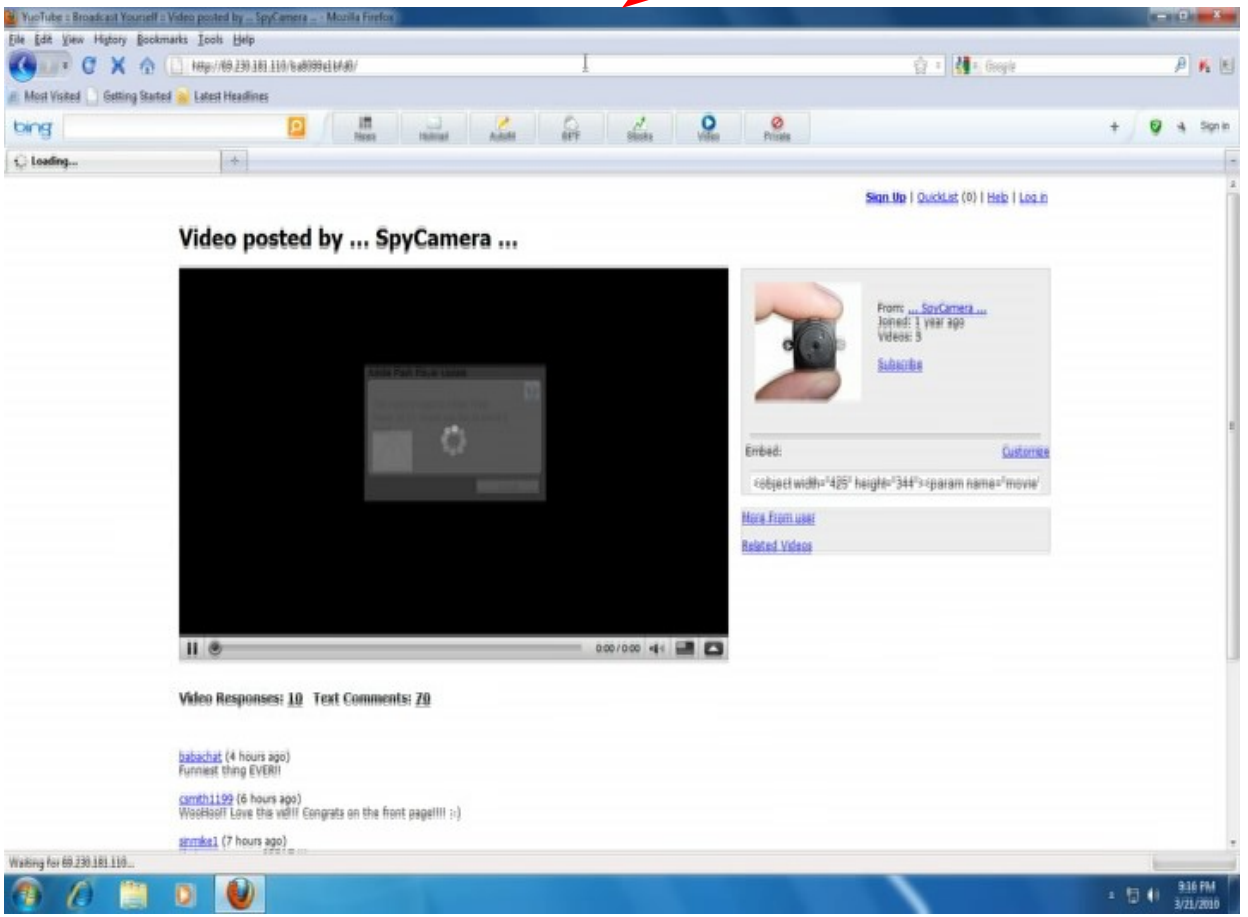
```
... (beginning code snipped)...
var b41bca = [
'94.16' + '9.6.105',
'77.78.' + '169.72',
'201.2' + '20.78.171',
'81' + '.57.237.246',
'65.32' + '.70.169',
'68' + '.146.40.37',
'6' + '8.80.92.193',
'89.1' + '76.106.238',
'82' + '.13.162.180',
'75.' + '228.54.56',
'84.22' + '0.234.190',
'69.201' + '.132.169',
'65.3' + '2.181.175',
'201.1' + '64.107.134',
'82' + '.228.220.165',
'65' + '.33.118.48',
'62.' + '72.251.182',
'99.234' + '.232.6',
'7' + '9.107.30.47',
'68.' + '62.21.71',
''];
... (a lot more code snipped)...
```




The Javascript code tells your browser to try to connect to each of these 20 computers.

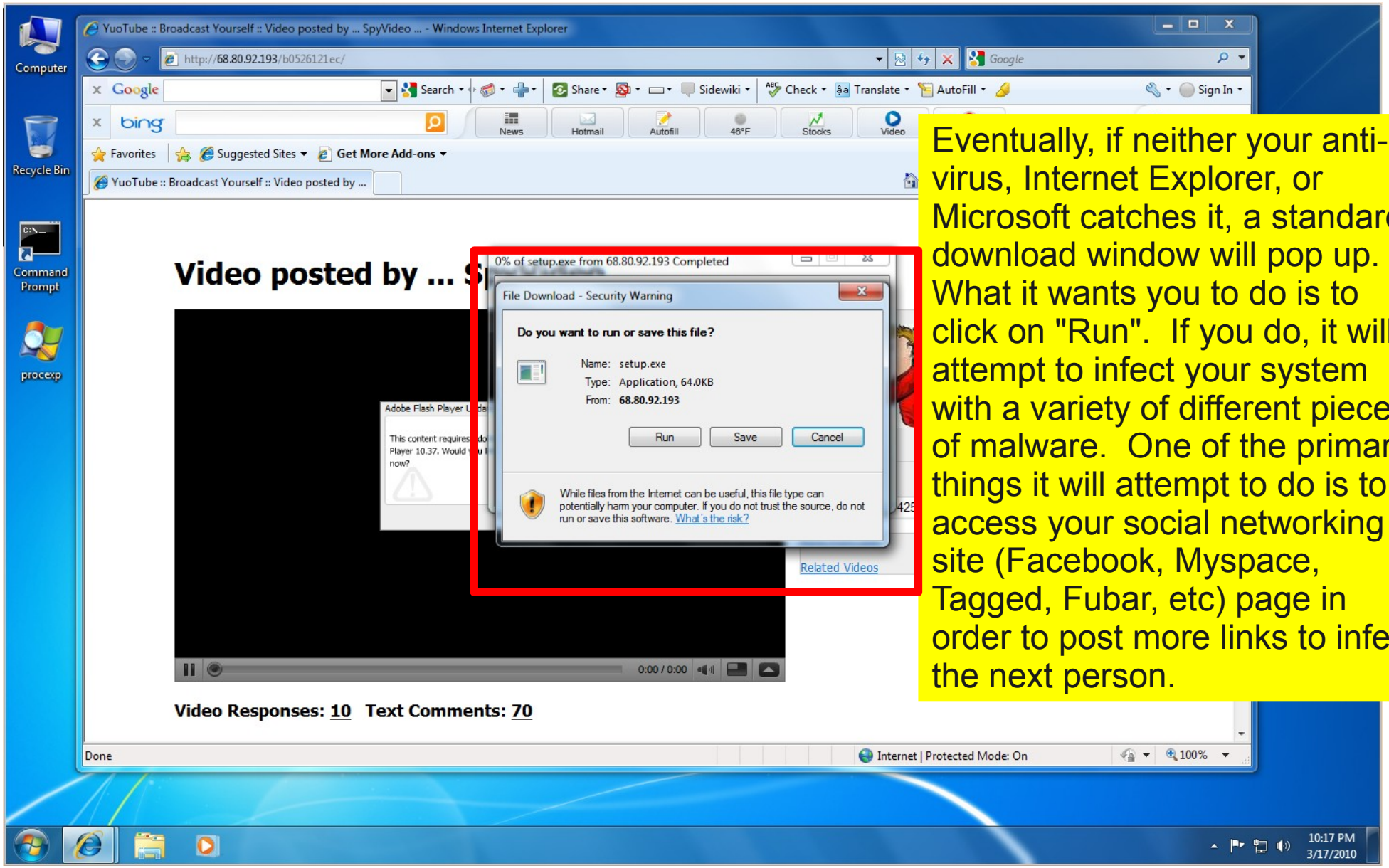
**NOTE: It's possible that most of these 20 IP addresses are fake and are meant to provide more obfuscation.**

68.80.92.193 → **Hello!** → ... here's some more Javascript code I want you to run.



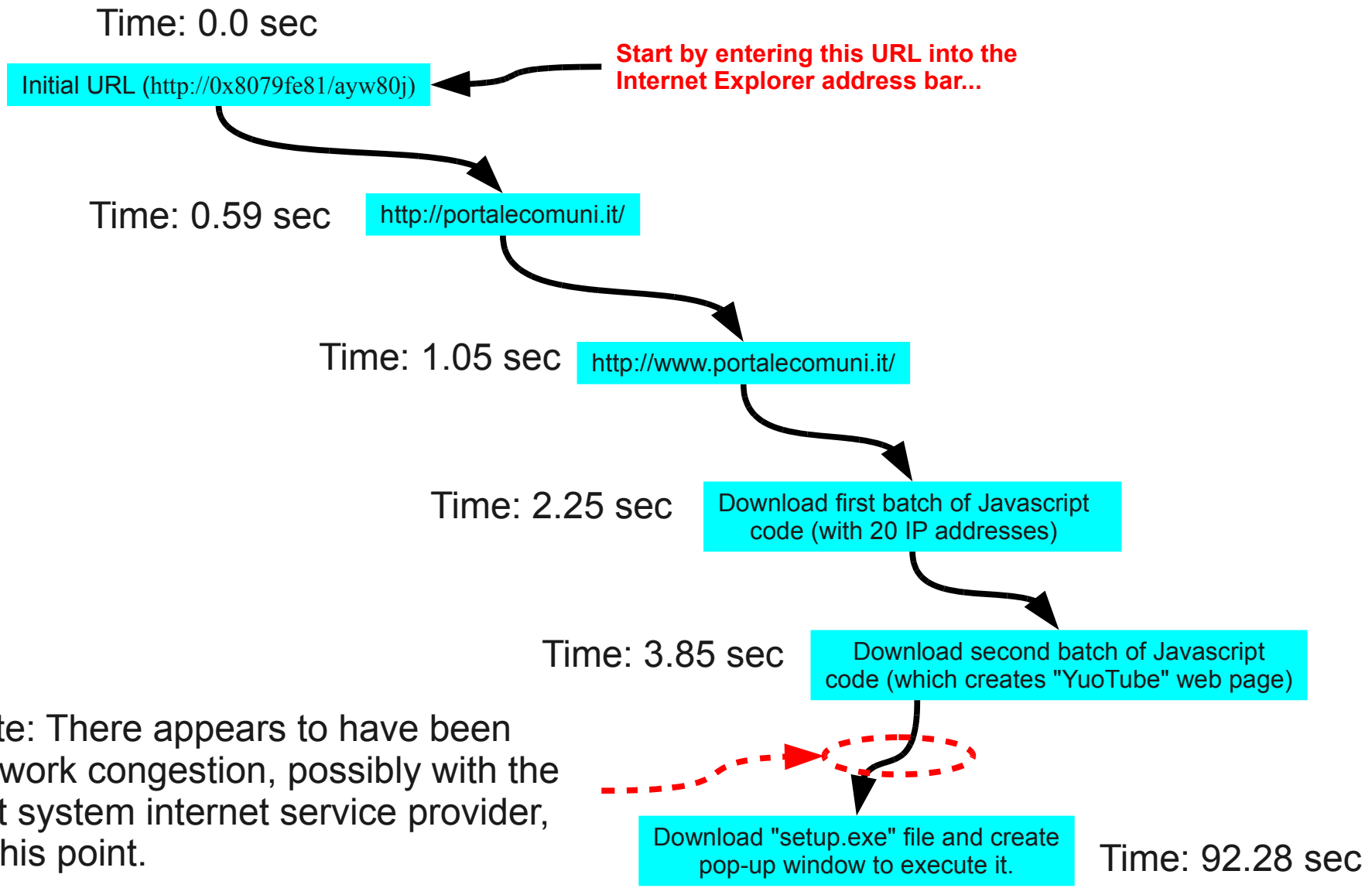

The new Javascript code starts by looking at whether you are running Internet Explorer or Opera (those are the only two that it seems to check for) and/or Windows. It then creates this fake YouTube (note that it's name is listed as "YuoTube") and tells you that you need to download a Flash Player upgrade.

# The Beginning of the End



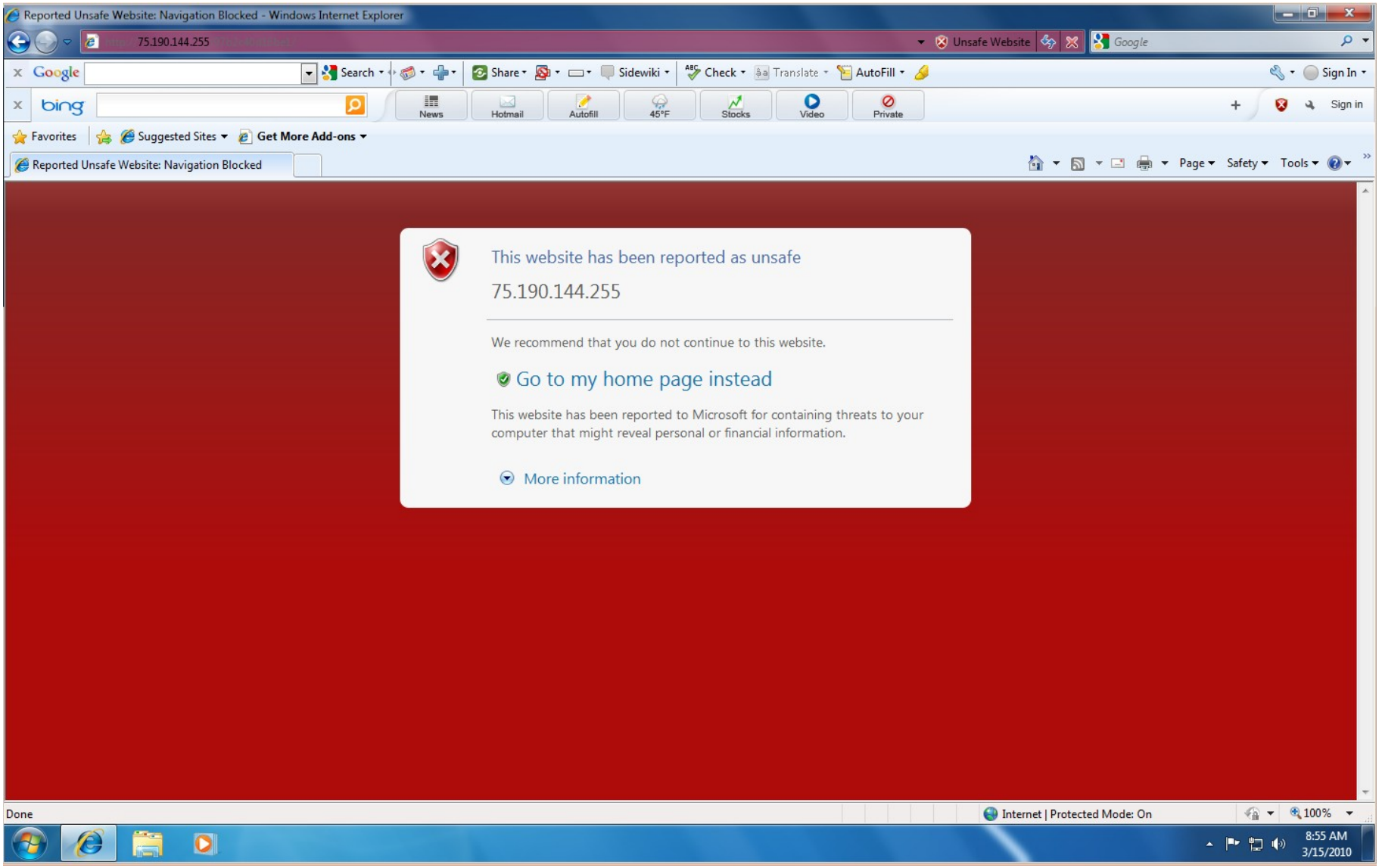

Eventually, if neither your anti-virus, Internet Explorer, or Microsoft catches it, a standard download window will pop up. What it wants you to do is to click on "Run". If you do, it will attempt to infect your system with a variety of different pieces of malware. One of the primary things it will attempt to do is to access your social networking site (Facebook, Myspace, Tagged, Fubar, etc) page in order to post more links to infect the next person.

# Timeline



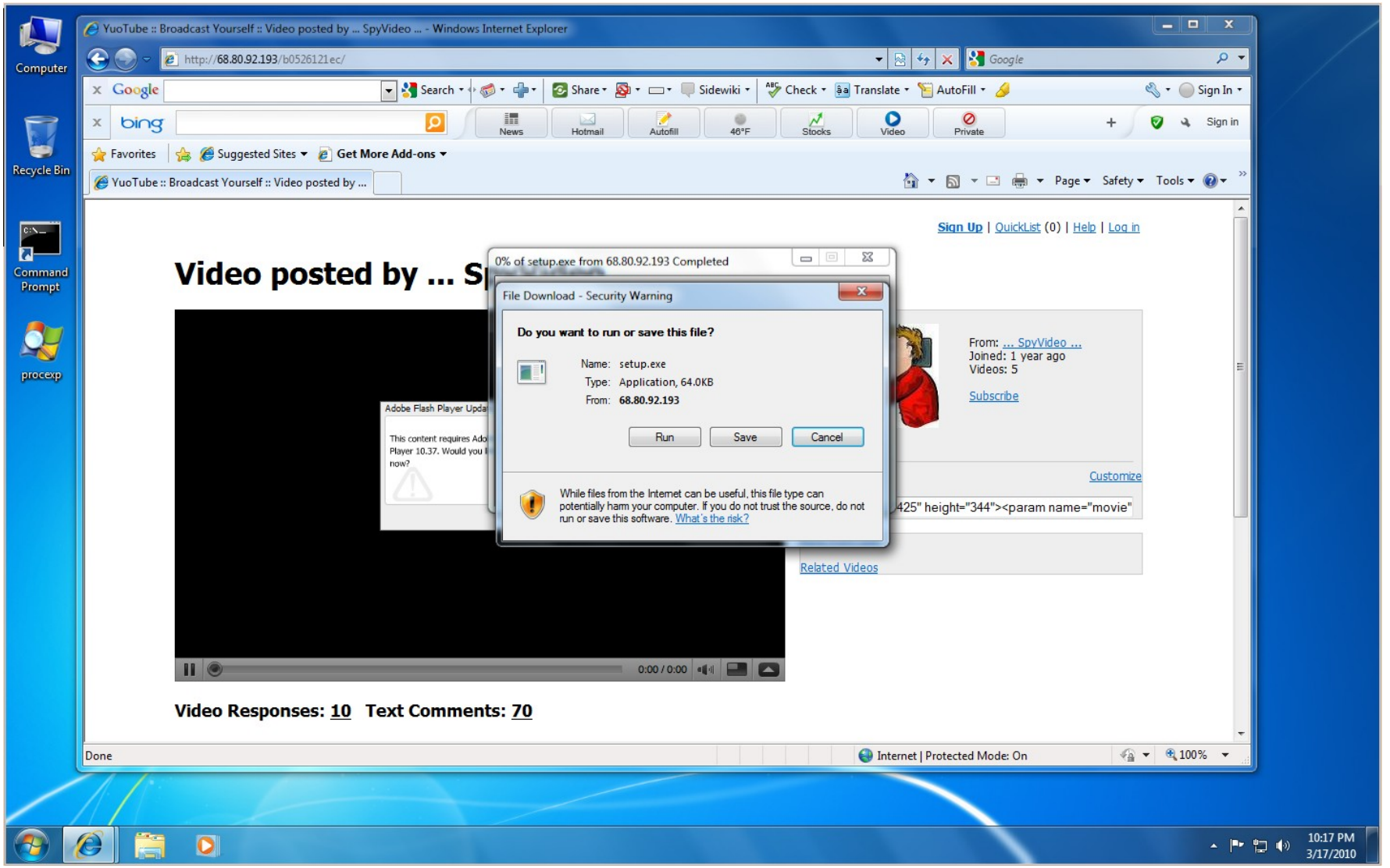

Note: There appears to have been network congestion, possibly with the test system internet service provider, at this point.

# Results of Different Attempts - Attempt #1



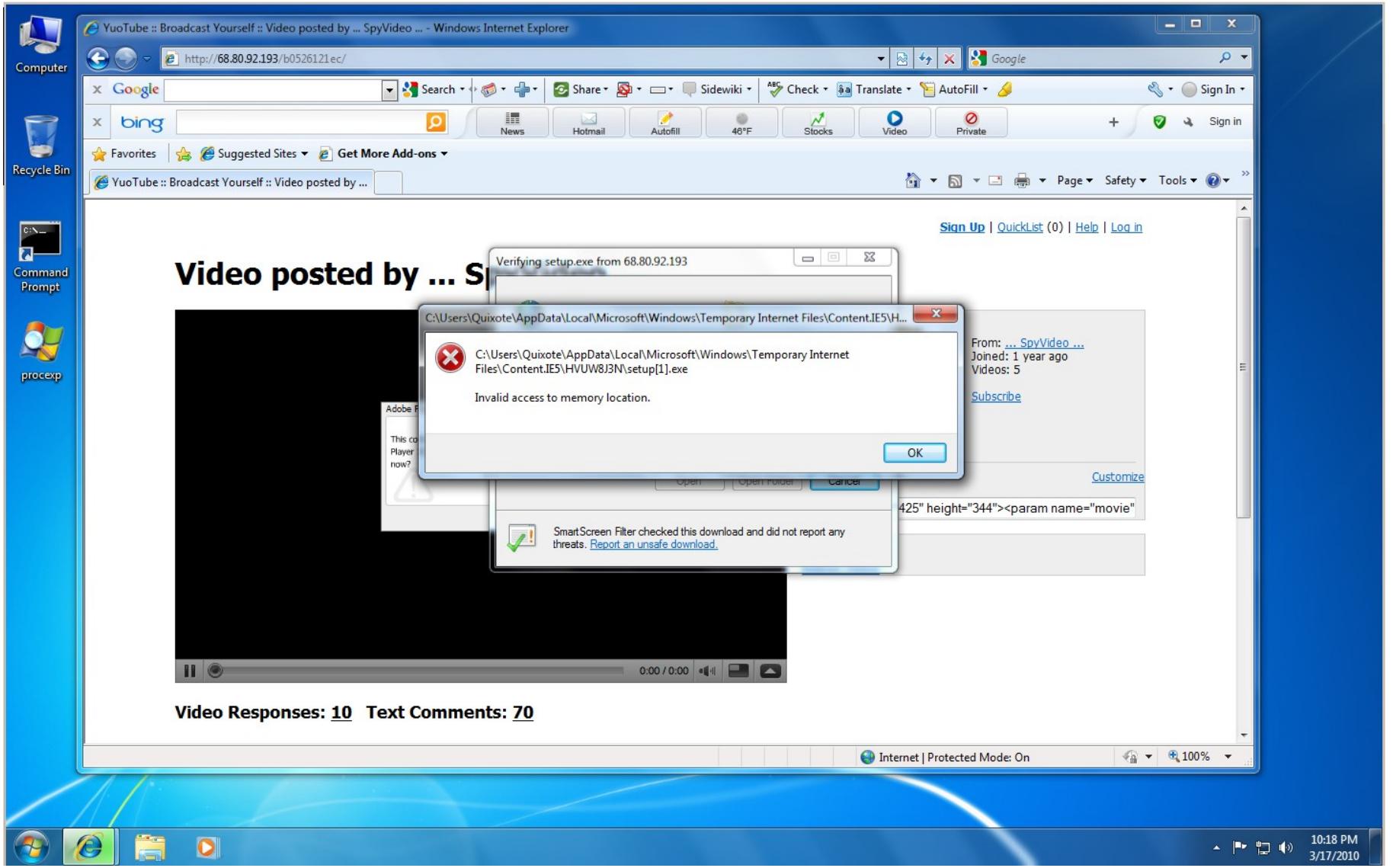

The first attempt using Internet Explorer went to one of the infected PCs that Microsoft appears to have already tagged as infected.  It stopped the access before the web page was brought up.

# Results of Different Attempts - Attempt #2



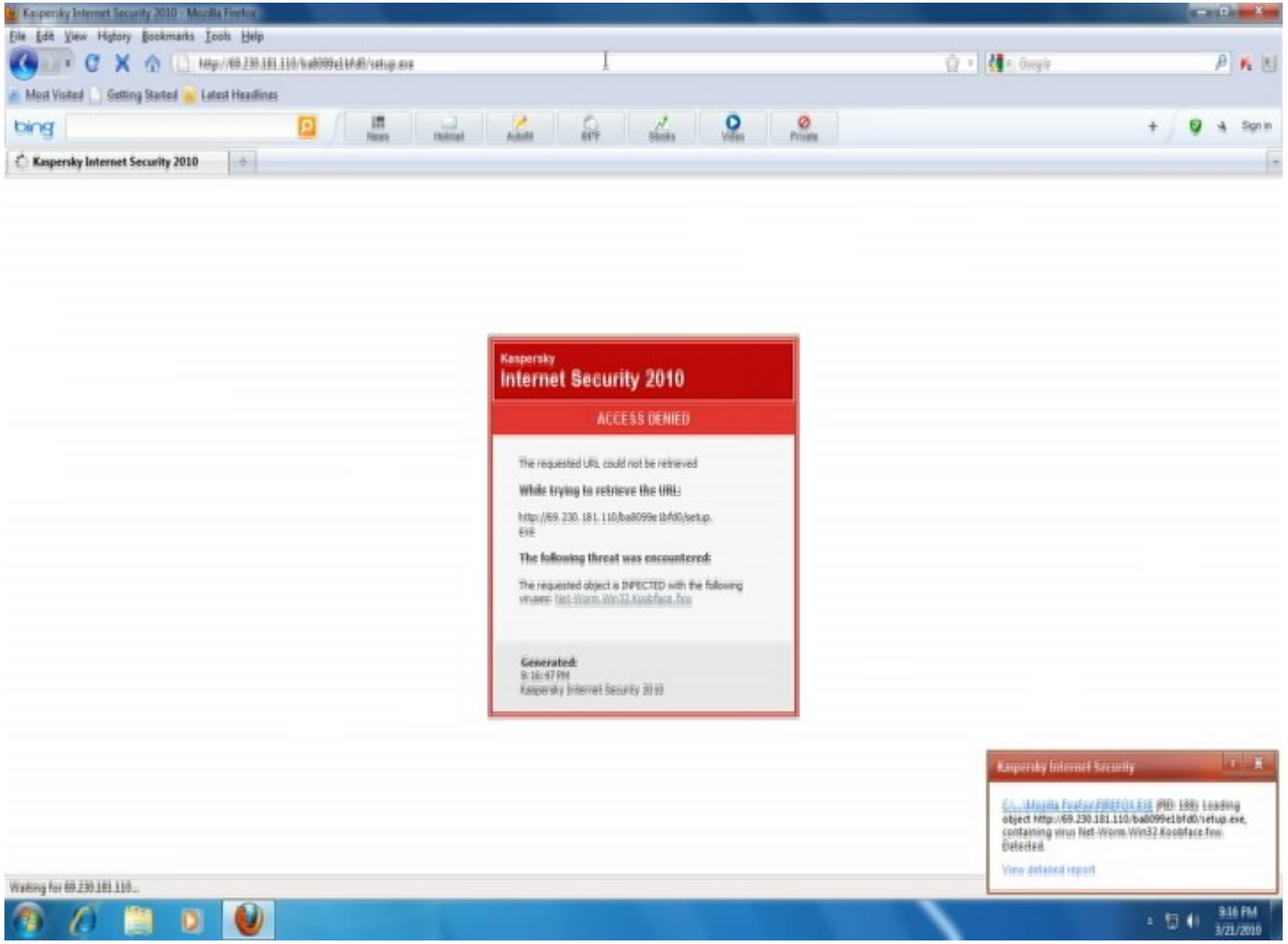

The second attempt using Internet Explorer went to one of the infected PCs that Microsoft appears to have NOT tagged as infected. The web page went up without a problem and the download file pop-up came up without any problems.

# Results of Different Attempts - Attempt #2




During the second attempt, I went ahead and clicked on "Run". A few seconds later, this window popped up stating it could not run the file. According to a Google search for the error message provided ("Invalid access to memory location"), the one consistent reason for this error was that the program did not have the privileges it wanted to run amok. Since this test was performed from a Windows 7 "limited" account, it appears that that kept the beast from breaking down the door and wreaking its havoc.

# Results of Different Attempts - Attempt #3




For the third attempt, I used Firefox rather than IE. When I did, I received this message from Kaspersky stating this web site was attempting to infect my computer. At first, I thought that perhaps Internet Explorer was not allowing Kaspersky to work since I'd visited the site twice before, both without any intervention from Kaspersky. However, a check of the Kaspersky web site showed that, between attempts #2 and #3, the Kaspersky virus signature database had finally updated to include the signature from this malware. A fourth attempt with IE also brought up this warning from Kaspersky.

# Results Summary

1) **No infection of Windows 7 appears to have taken place. This is based on a lack of problems with the system afterwards, plus several 10+ hour packet captures from Wireshark after each attempt.**

2) The three reasons that infections failed were:

   a) Microsoft has a database of known bad sites. Any attempt to access such a site with Internet Explorer will be stopped.

   b) The limited account does not have the privileges that this particular infection required to infect the system, despite the fact that it made it past both the Microsoft web site filter and Kaspersky antivirus filters to the point where I clicked on "Run".

   c) On the third access attempt, Kaspersky provided a warning that the site was attempting to infect the system. The reason it didn't on the first two was that Kaspersky did not yet have the signature of this particular piece of malware in its database. By the third attempt, it did.

3) This infection attempt required three servers and at least one other system that I believe was a personal computer that had been infected and become part of a botnet.

4) The first Javascript looks at the "referer" site, meaning the web site from which the link was derived, for some purpose. Since the link was not selected while in a social networking site, such as Facebook.com or Myspace.com, it's unknown what the result would be.

# Results Summary (cont)

5) If the hypothesis is correct that the systems included as part of the 20 random IPs within the first batch of Javascript code, this could be a form of separation between the people controlling the botnet and the actual malicious code, all of which resided on these computers. The first three servers merely redirected traffic; they did not attempt to infect visiting systems.
6) The systems that were part of the 20 IPs in the first batch of Javascript code have been checked using "whois". They come back as systems which are typically small to midsize ISPs, such as Comcast and Road Runner in the US, Rogers Cable in Canada, and Tellas.gr in Greece.
7) **The people controlling this system are only interested in Windows-based systems. Any attempt to access the system using Linux-based systems will be ignored and simply redirected to a Russian-based web site that offers downloadable videos.**