TippingPoint Digital Vaccine Laboratories
Contact Us
DVLabs Logo
Navigation

1. About
2. Team
3. Blog
4. DVLabs Advisories
5. DVLabs Upcoming Advisories
6. DVLabs Published Advisories
7. Appearances
8. Resources
9. Zero Day Initiative
10. RSS

DID YOU KNOW... In December of 2007, Microsoft released seven security bulletins which fixed 11 new security vulnerabilities. TippingPoint and ZDI were credited with discovering a total of four of those vulnerabilities.

- ▼ 2013
  - ► January (2)
    - (loading)
- ► 2012
  - ► October (1)
    - (loading)
  - ► July (1)
    - (loading)
  - ► June (1)
    - (loading)
  - ► May (1)
    - (loading)
  - ► April (2)
    - (loading)
  - ► March (1)
    - (loading)
  - ► February (5)
    - (loading)
- ► 2011
  - ► December (4)
    - (loading)
  - ► November (1)
    - (loading)

- ► October (1)
  - (loading)
- ► September (1)
  - (loading)
- ► July (2)
  - (loading)
- ► June (1)
  - (loading)
- ► May (1)
  - (loading)
- ► April (3)
  - (loading)
- ► March (1)
  - (loading)
- ► February (12)
  - (loading)
- ► January (1)
  - (loading)

• ► 2010
- ► December (1)
  - (loading)
- ► November (1)
  - (loading)
- ► October (1)
  - (loading)
- ► September (4)
  - (loading)
- ► August (1)
  - (loading)
- ► July (1)
  - (loading)
- ► March (1)
  - (loading)
- ► February (2)
  - (loading)

• ► 2009
- ► October (1)
  - (loading)
- ► September (3)
  - (loading)
- ► July (1)
  - (loading)
- ► June (5)
  - (loading)
- ► May (1)
  - (loading)
- ► April (2)
  - (loading)
- ► March (9)
  - (loading)
- ► February (7)

- (loading)
- ► January (5)
  - (loading)
- ► 2008
  - ► December (2)
    - (loading)
  - ► November (4)
    - (loading)
  - ► October (7)
    - (loading)
  - ► September (9)
    - (loading)
  - ► August (16)
    - (loading)
  - ► July (9)
    - (loading)
  - ► June (11)
    - (loading)
  - ► May (1)
    - (loading)
  - ► April (4)
    - (loading)
  - ► March (6)
    - (loading)
  - ► February (4)
    - (loading)
- ► 2007
  - ► December (1)
    - (loading)
  - ► November (5)
    - (loading)
  - ► October (4)
    - (loading)
  - ► September (1)
    - (loading)
  - ► August (2)
    - (loading)
  - ► July (9)
    - (loading)
  - ► June (4)
    - (loading)
  - ► May (8)
    - (loading)

Filtering Content: Online Web Proxy Detection

- By Derek Brown
- Sat 30 May 2009 13:20pm
- 11172 Views
- 1 Comments

- Link

As of late, we have seen a fairly significant number of customer requests for filters that block access to free online proxy websites. Those of you who subscribe to our Digital Vaccine service have probably noticed the influx of filters addressing these requests; I thought you might find it interesting to understand just how it is that we are able to cover such a wide swath of websites with a relatively small filter set.

One of the easiest ways to evade URL or IP based filtering is to use a proxy. A proxy is third-party server that acts on the requestor's behalf to download content from the Internet. One method of proxied content delivery that is growing in popularity is online web proxies or CGI-based proxies. These services are written in a scripting language, usually PHP or Perl, and hosted on a public web server. A few of the most popular are PHProxy, CGIProxy, and Glype. Applications such as these allow users to proxy the download of their content in a point-and-click fashion instead of having to locate an anonymous proxy server somewhere on the internet, plug in the server IP address and port into their web browser, and repeat the process until they find a working one.

Suppose, for example, that the network administrator of your company thinks you should not be performing any type of searches through Google; most likely, she would implement a URL-based rule disallowing her users from visiting the site. This is where proxies become a perfect solution because the users don't have to actually visit Google's site to view its content. The way CGI-based proxies work is that the user visits a site that hosts the software such as ProxyBoxOnline, which hosts the Glype software, and type "google.com" into the URL form, then hit enter and perform searches till their heart’s content without the worry of being blocked.

All of these pieces of software perform the same function but behave in slightly different ways. Typing “google.com” into the URL form at ProxyBoxOnline and clicking “GO” causes the following request to be made:

```
POST /includes/process.php?action=update
HTTP/1.1 Host: www.proxyboxonline.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.proxyboxonline.com/
Cookie: s=cn03fdpa2n5u6m7edl1eiqnr54;
__utma=256566602.3147972642932281300.1243628807.1243628807.1243628807.1; __utmb=256566602.1.10.1243628807;
__utmc=256566602; __utmz=256566602.1243628807.1.1.utmcsr=proxy.org|utmccn=(referral)|utmcmd=referral|utmcct=/
Content-Type: application/x-www-form-urlencoded
Content-Length: 52
u=google.com&encodeURL=on&allowCookies=on&stripJS=on
```

In this request, you can see the URL in the post data as well as a few software level options that are turned on. The server responds with the following redirect:

```
HTTP/1.1 301 Moved Permanently
Date: Fri, 29 May 2009 18:24:02 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Cache-Control: public, max-age=2592000
Last-Modified:
```

```
Expires: Sun, 28 Jun 2009 18:27:01 GMT
Location: http://www.proxyboxonline.com/browse.php?u=Oi8vd3d3Lmdvb2dsZS5jb20v&b=13
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

In turn, the browser makes the following request:

```
GET /browse.php?u=Oi8vd3d3Lmdvb2dsZS5jb20v&b=13 HTTP/1.1
Host: www.proxyboxonline.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1;en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.proxyboxonline.com/
Cookie: s=cn03fdpa2n5u6m7edl1eiqnr54 __utma=256566602.3147972642932281300.1243628807.1243628807.1243628807.1;
__utmb=256566602.1.10.1243628807; __utmc=256566602; __utmz=256566602.1243628807.1.1.utmcsr=proxy.org|utmccn=
(referral)|utmcmd=referral|utmcct=/
```

What is returned from the server is a slightly modified Google home page. The way it works is pretty simple: the server base64 encodes the URL in the first request, along with encoding the options we have chosen, into a single number and redirects to the file browse.php with these options as parameters. When the browser makes the request to browse.php the server-side software decodes the URL and fetches the content for us. Once it grabs the content, it modifies all tags referring to Google and points them back to itself. Got that? No? Ok, well, here is an example using the infamous Google logo image:

Here is what the tag looks like when normally accessed

```
<img alt="Google" height=110 src="/intl/en_ALL/images/logo.gif" width=276 id=logo onload="window.lol&&lol()">
```

Here is what the tag looks like when accessed through ProxyBoxOnline

```
<img alt="Google" height=110 src="http://www.proxyboxonline.com
/browse.php?u=Oi8vd3d3Lmdvb2dsZS5jb20vaW50bC9lbl9BTEwvaW1hZ2VzL2xvZ28uZ2lm&b=13" width=276 id=logo >
```

Notice the difference? If we base64 decode the u parameter, then we get the source URL we expected to see

```
Oi8vd3d3Lmdvb2dsZS5jb20vaW50bC9lbl9BTEwvaW1hZ2VzL2xvZ28uZ2lm --> ://www.google.com/intl/en_ALL/images/logo.gif
```

Since our browser never actually visits google.com the URL-based rule is pretty much worthless at this point. So why not just create a URL rule for www.proxyboxonline.com? Because this software is open source, anyone can easily download it and host it on a public web server with only a few clicks. In other words, your network administrator would be forced into a perpetual game of “whack-a-mole” – chasing new proxy websites as fast as they appear and causing the URL rules to be constantly updated.

For more information on the number of freely available proxy software distributions, try the popular proxy.org repository here. TippingPoint Digital Vaccine subscribers can view the online web proxy filter set described by filters 5195, 5199, 5201, 5871, 6917, 6903, 6873, 6879, 6880, 6881, 6882, 6910, 6898 and 6905.

Tags:
Published On: 2009-05-30 13:20:18

Comments **post a comment**

1. Mark S. commented on 2009-05-31 @ 08:41

   Great article...proxy avoidance is absolutely one of the premier threat vectors of the day. I say threat vector for obvious reasons...it's not just obscuration...it's another way for users to make common mistakes, but "undetected" by the administrator/mechanisms that may/may not be in place.

   Even more so troubling, though, and a bit tougher to deal with, are the reflectors/anonymizers via SSL. Same deal, different transport...that transport being encrypted, that is. Take any of the popular proxy avoidance sites, add a little "s" to the end of http, and all of a sudden, you've got a new weapon in the battle.

   Take comfort, though...there are tools out there to deal with SSL anonymizers/reflectors, too, though...just be aware that they exist, and that your current tools have no visibility. You've got to terminate SSL to get true visibility, and while that brings many privacy issues to front, the fact is corporate assets are just that...so minimize that argument, and deal with the threat that is SSL...

Trackback

RSSPublished Advisories

TPTI-12-05: Oracle
- published 2012-06-29

TPTI-12-06: Hewlett-Packard
- published 2012-06-29

TPTI-12-04: Samba
- published 2012-06-29

TPTI-12-03: Adobe
- published 2012-04-18

TPTI-12-02: Novell
- published 2012-03-22

RSSUpcoming Advisories

HP
- reported 2013-01-07

HP
- reported 2013-01-07

EMC
- reported 2012-03-14

Novell

- reported 2012-03-14

EMC

- reported 2012-02-22

RSSBlog Entries

Pwn2Own 2013

- 2013-01-17 by Brian Gorenc
- *(0 Comments)*

2012: Year in Review

- 2013-01-08 by Brian Gorenc
- *(0 Comments)*

EUSecWest Mobile Pwn2Own 2012 Recap

- 2012-10-05 by Brian Gorenc
- *(0 Comments)*

Mobile Pwn2Own 2012

- 2012-07-20 by Brian Gorenc
- *(0 Comments)*

ZDI Update – June 2012

- 2012-06-22 by Assad Khan
- *(0 Comments)*