

[Full-Disclosure] DANGER ZONE: Internet Explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-12/0747.html>

http-equiv_at_excite.com

Date: 12/26/03

To: <full-disclosure@lists.netsys.com>

Date: Fri, 26 Dec 2003 17:02:55 -0000

Friday, December 26, 2003

Technical 'silent delivery and installation of an executable on a target computer. No client input other than viewing and web site'. This may be achieved with the Internet Explorer series of so-called "browsers", all security settings set to HIGH !

[***premium advertising space: your ad here for a nominal monthly fee contact sales@malware.com***]

Not so simple:

The current trend is to dismiss, pooh pooh, the never-ending ongoing [almost daily] discoveries of vulnerabilities in the Internet Explorer series of browsers. So much so there remains in the account a balance of several full and complete remote compromises [courtesy of: Liu Die Yu

http://www.safecenter.net/UMBRELLAWEBV4/DirSvc/security/originality/microsoft_ie/index.html] summarily dismissed as "well the internet is a big bad place, don't surf to unknown sites, and sites you do know and trust, place in the Trusted Zone. You'll be fine. "Trust Us !"".

Oh. Okay:

The so-called "Trusted Site" zone setting in the Internet Explorer series of browsers, is set to LOW on default [screenshot: <http://www.malware.com/trustus.png> 28KB]. What that means is 'minimal safeguards and prompts are provided...most content is downloaded and run without prompts'. So who do [can] we trust?

For example, we input into the so-called Trusted Zone, the manufacturer commonly known as Microsoft Dot Com [screenshot: <http://www.malware.com/havefaith.png> 15KB]. In fact this peculiar method and remedy of participating in the World Wide Web is recommended by the brains behind the the manufacturer commonly known

as Microsoft Dot Com.

Now what:

There is a small yet critical bug in the mailing list software called LISTSERV from <http://www.lsoft.com/>. A trivial yet important ability to effect the common so-called 'cross site scripting' [see: <http://www.cert.org/advisories/CA-2000-02.html>] 'malicious html tag embedding in client web requests':

Microsoft.com uses the mailing list software called LISTSERV. So do some 300,000 combined public and local others [Note: These numbers do not include Intranet servers]. Banks. Governments. Schools etc [see: <http://www.lsoft.com/customer/clientlist.asp>].

So:

So what that means is if we 'trust' our government, or trust our bank or our school or even our software 'manufacturer', we are advised to place everyone else in the 'restricted zone' and our trusted sites in the 'trusted zone' where: 'minimal safeguards and prompts are provided...most content is downloaded and run without prompts'.

Example:

[http://discuss.microsoft.com/SCRIPTS/WA-MSD.EXE?A0=%20SRC=javascript:document\['write'\]\(location\)>&T=malware is in the zone<object>](http://discuss.microsoft.com/SCRIPTS/WA-MSD.EXE?A0=%20SRC=javascript:document['write'](location)>&T=malware is in the zone<object>)

<http://lists.state.gov/SCRIPTS/WA-USIAINFO.EXE?A1=ind0312d&L=dosback>

<http://demo.lsoft.com/Scripts/wa-demo.exe?A1=ind9807&L=demo>>

What that means is we can install via `<object classid="" codebase="">` any executable file from within the same domain as we see fit. The same domain in the so-called 'Trusted Site' zone that is. Be it *.gov. *.microsoft.com, *.edu et cetera.

Technically our codebase cannot point to a remote site outside the zone as it will be cached in the Temporary Internet File [TIF] and will prompt for install as that remote site is in the Internet Zone. However, theoretically we can play havoc within our *.gov and .edu domains on one another. More importantly, we might very well be able to write our entire Self-Executing HTML file into all of these domains:

MIME-Version: 1.0
Content-Location: file:///malware.exe
Content-Transfer-Encoding: base64

Full-Disclosure: [Full-Disclosure] DANGER ZONE: Internet Explorer

```
TVpEAQUAAgAgACEA//91AAACAACZAAAAPgAAAAEA+
zBqcgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAB5AAA
AngAAAAAAAAAAAAAAAAAAA=/www.malware.com//
<object CLASSID="CLSID:5 5 5 5 5 5 - 5 5 5 5"
code base="mhtml:'+path+'">
```

In which case the entire package will be cached in the TIF under the disguise of a so-called 'TRUSTED ZONE' !

Don't trust us. Trust them.

[***less than premium advertising space: your ad here for a nominal monthly fee contact sales@malware.com***]

Happy New Year and be safe out there. It's not what it all seems.

End Call

--

<http://www.malware.com>

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>