FEATURE 2

HaTeMaiL EMAIL!

Martin Overton
Independent researcher, UK

George Santayana is credited with the following statement:

> 'Those who cannot learn from history are doomed to repeat it.'

And David C. McCullough with the following statement:

> 'History is a guide to navigation in perilous times. History is who we are and why we are the way we are.'

How can we possibly understand risks and threats if we fail to look at their history, and more importantly, learn from it?

With this in mind, let us look back, before looking forward once more.

IN THE BEGINNING ...

> 'I remember the good old days when all email was plain ASCII and to indicate that something was in bold you put a * either side of the word you wanted to emphasize. There were no different-sized fonts, no colours, and no inline pictures (unless they were made up of ASCII characters) ...
>
> 'And then some bright spark decides it would be a good idea to use this new-fangled format called HTML [HyperText Markup Language] ...
>
> 'Pah! Using HTML for email instead of good old plain ASCII, it's just asking for trouble ... it'll all end in tears, mark my words ...'

No, that wasn't me, but it's a common view among those of us who have been in computing a few decades and grew up using the fledgling internet; we who cut our teeth on ASCII email, FTP and NNTP, as well as the more advanced tools available at the time, such as Gopher and WAIS.

I don't use HTML-based email unless I have to, as I still prefer to use plain ASCII. Call me old-fashioned if you wish, but at least I know that there are no nasty HTML exploits in my email, or embedded scripting languages that will be executed when I read the email. No web-bugs, no remote graphics are loaded, unless I want them to be.

LEARNING TO LOATHE

HTML email does more than deliver pretty stationery, clickable links and pictures to our inboxes. It can be the way in which your system becomes infected or how an advertiser or spammer/scammer knows you have opened/viewed the email.

Not convinced that HTML in email is inherently 'bad' and should be considered HaTeMaiL? Well, let me try and show you a number of malicious examples to see if I can convince you.

First I will cover a couple of historical incidents, and then we will move on to more recent times.

BURSTING THE BUBBLE

VBS/BubbleBoy [1] was the first worm that was able to spread via email without requiring the recipient to open (launch) an attachment.

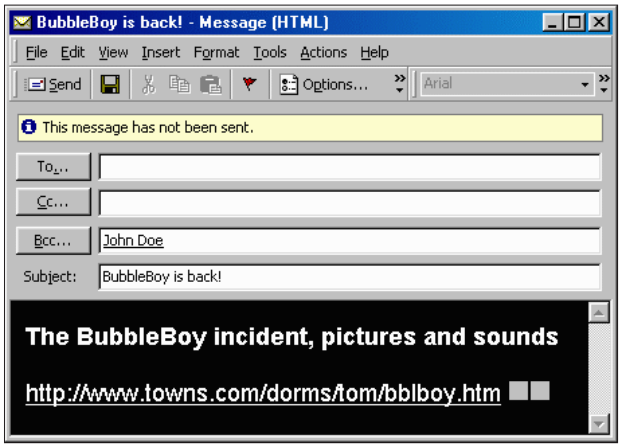

Figure 1: BubbleBoy email. Image courtesy of F-Secure.

Simply rendering/viewing the email in vulnerable versions of *Outlook* will infect a vulnerable system. Scripting can be embedded in HTML-based email so that the script is run automatically when the mail is rendered, and unless you look at the raw email source you won't even know it is there!

BubbleBoy then goes on to modify the owner registration details for the copy of *Windows* that it has just infected to show it registered to 'BubbleBoy, Vandelay Industries'.

Finally, it mass-mails a copy of itself in a similar fashion to Melissa [2].

IT'S ALL KAK

Kak [3] is a worm that, like BubbleBoy, embeds itself into every email sent from the infected system, without any attachment.

Just like BubbleBoy, it infects a vulnerable system on previewing or opening the email, no clicking or double-clicking required as there is no attachment.

Kak is written in JavaScript and it works on both English and French versions of *Windows 95/98* if *Outlook Express*

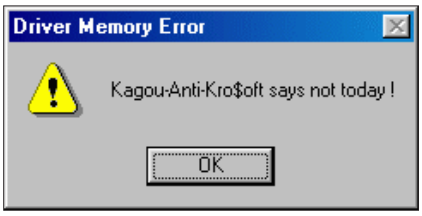

Figure 2: Kak payload message, image courtesy of F-Secure.

5.0 is installed. It does not work in a typical *Windows NT* installation.

The worm triggers on the first day of each month, but only if the system time is later than 18:00. When it triggers it shows the message seen in Figure 2 and then proceeds to shut down *Windows*.

Now let's move on to the more recent uses of HTML in email.

GREETINGS!

One of the current uses of HTML email by malware authors is sending out fake e-cards (electronic greetings cards) to attempt to get people to infect themselves via a social-engineering trick.

The following are a few examples of the fake e-card HTML emails I've seen recently:

Figure 3 shows a professional-looking HTML email, which may very easily be mistaken for a real e-card by an intended victim.

Figure 4 shows an HTML email which uses one of the most successful social-engineering techniques employed by malware authors.

Figure 5 shows another well thought out fake e-card notification, which even mentions that the e-card is a *Flash* executable, thus increasing the chances that the intended target will run the file without another thought.

Of course, each of these lead not to a card but to a malicious file, usually a trojan.

Probably the cleverest example I have seen so far this year was a fake Valentine's Day card which prompted the recipient to install a fake plug-in (malicious software disguised as a *Flash* plug-in) when they visited the website to retrieve their e-card. The clever part was that the prompt to install the 'plug-in' was only displayed the first time the user visited the site – on any return visits the user would simply see a real e-card. More details can be found in [4].

The next section deals with another interesting email that not only uses social engineering but also exploit code. Like

Figure 3: Fake Hallmark e-card email.

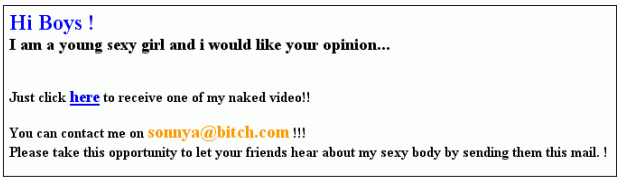

Figure 4: Fake Greetings.com e-card email.

Figure 5: Fake 2000Greetings.com e-card email.

BubbleBoy and KAK, the exploit code will trigger on unpatched systems when the email is opened or previewed on most email clients, not just *Outlook*.

Swen [5] arrives as a very professional-looking HTML email claiming to be from *Microsoft* and warning of a new virus on the loose. The warning email just happens to include the 'patch' to stop the virus; how kind of them to send it out to all their customers! Of course, the patch is, in fact, the virus and the email didn't come from *Microsoft* at all.

Maybe you now see why it is important to look back, as many tricks/techniques are rediscovered, dusted off and reused.

PRETTY, BUT DANGEROUS

Don't look ... I told you not to look!

Figure 6: Paris Hilton WMF email screenshot.

Too late, if the screenshot shown in Figure 6 was an email you had previewed or opened on your system, and you hadn't patched or had other mitigating technologies or methodologies in place (such as a good, up-to-date, and enabled, anti-malware solution and/or fully patched system or one not using *Windows*), then your computer would now be infected. Yes, you would be '0wn3d'.

I have doctored the screenshot, since the real one is a little too risqué to display here. The first picture, the one of 'Paris Hilton' barely wearing anything, is not 'bad'. What I mean is that the picture itself is not the problem in this email, it is simply the bait. The one to worry about is the second picture, which won't render (the one with the red diamond in the screenshot), because it isn't a real picture at all. It is a trojanised Windows MetaFile (WMF), which has exploit code embedded in it to try and infect or take over your computer.

So, why am I writing about this now? I mean, the exploit code used is old, and you should all be patched by now.

The reason I'm flagging this is that I believe that there will be a new phase of 'image' exploitation (in both senses of the word) such as this one using the 'WMF exploit'. I suspect we will see the same social-engineering techniques used with other exploit code and droppers. In fact, I know we will!

ANI EXPLOIT WILL DO

It is not the first time that Paris Hilton has been used as an incentive to exploit *Windows* vulnerabilities. At the beginning of April, pictures of the Hilton heiress as well as pictures of Jenna Jameson and Britney Spears were used as bait for potential victims of the .ANI vulnerability (see *VB*, May 2007, p.4).

CONCLUSIONS

If you haven't already, I would strongly suggest that you set your email program not to render HTML automatically or to download remote graphics. Most modern email clients now have this as a default setting.

If you must use HTML-based email, then please be careful when opening or even previewing HTML emails, as you may start a chain reaction which ends up with your system being turned into a zombie, or worse, and it's all downhill from then on.

There are numerous reports [6] that people are abandoning email as a communication medium. It is claimed that this is mainly due to spam and malware. Certainly statistics from my personal mail server show that in May 2007 over 91% of the mail I received was unsolicited. This is the highest percentage I have seen since I started collating this data at the start of 2004.

So, let me now play devil's advocate, how many of you reading this article agree with the following?

- HTML email was an accident waiting to happen.
- HTML has no real place in emails at all.
- HTML should stay on web pages where it was always meant to be.

And a final question for you:

- Is the reputation of email now so badly damaged that it can never recover the relative trust it once had?

Please send answers to me on a postcard (e-card), a real one that is. Let the flame-fest begin!

REFERENCES

[1] A full description can be found at http://www.f-secure.com/v-descs/bubb-boy.shtml.

[2] A full description can be found at http://www.f-secure.com/v-descs/melissa.shtml.

[3] A full description can be found at http://www.f-secure.com/v-descs/kak.shtml.

[4] http://momusings.com/momusings/2007/02/stupid-cupid-stop-picking-on-me.html.

[5] A full description can be found at http://www.f-secure.com/v-descs/swen.shtml.

[6] For example http://www.castlecops.com/a3794-Spam_pushes_many_to_stop_using_e_mail.html and http://www.symantec.com/press/2003/n031202a.html and http://www.crn.com/security/18842210.