

[Full-Disclosure] os x mass mailers

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-02/1082.html>

From: petard (petard_at_freeshell.org)

Date: 02/18/04

To: Joshua Levitsky <jlevitsk@joshie.com>

Date: Wed, 18 Feb 2004 19:59:50 +0000

On Wed, Feb 18, 2004 at 12:09:54PM -0500, Joshua Levitsky wrote:

> *Personally I hope someone is writing an OS X virus / worm to shut those
> people up about how secure the 3% using Macs are. How hard is it for someone
> to write a freaking osascript that tell application Address Book.app ... and
> then tell application Mail.app ... and you would have the same problems as
> windows. It would be nice to have a little less stress with Windows and let
> the others suffer for a while.*

the script to do so is trivial... certainly easier than on windows, I'd say. in fact, here's how to send a message with no user interaction at all in applescript, provided mail.app is running and authenticated to your server as required:

```
tell application "Mail"
```

```
    set newMessage to make new outgoing message with properties  
    {subject:"some witty subject", content:"some random garbage",  
    sender:"some@loser.tld" }
```

```
    tell newMessage
```

```
        make new to recipient at end of to recipients with properties  
        {name:"Victim", address:"victim@other.tld" }
```

```
        send
```

```
    end tell
```

```
end tell
```

The issue is getting that to propagate on a large scale. There are 3 problems:

1. Mail.app doesn't automatically execute incoming scripts.
2. If you ship it as a "script" (even run-only) the only thing that happens when someone double-clicks it is that script editor opens; it doesn't run. Most mac users have never seen the script editor, wouldn't like it, and would promptly quit.
3. If you ship it as an application bundle, mail presents a very dire warning about how you shouldn't open it because it may contain a virus or be harmful to your computer and does not default to opening it.

Those 3 issues assume you've hit an os x user who runs mail.app. Other users just wouldn't be able to execute it if they want and are stupid

Full-Disclosure: [Full-Disclosure] os x mass mailers

enough to do so. And that's most of the recipient pool. (95% of the people in a non-technical user's address book are likely to be windows users. Not exactly fertile ground for an applescript virus.)

The combination of more difficult social engineering thanks to a safer default configuration of the environment and a smaller user population make writing this mass mailing trojan very unrewarding. The upshot is that, as a practical matter, the 3% using Macs are much safer.

And you must just be an ass if you hope for more of this crap to clog your mailbox, whether you use the platform in question or not. I haven't been vulnerable to a single one of them, but they irritate me and I certainly don't want more stuff like it bogging down my servers.

regards,
petard

--

If your message really might be confidential, download my PGP key here:
<http://petard.freeshell.org/petard.asc>
and encrypt it. Otherwise, save bandwidth and lose the disclaimer.

Full-Disclosure - We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>