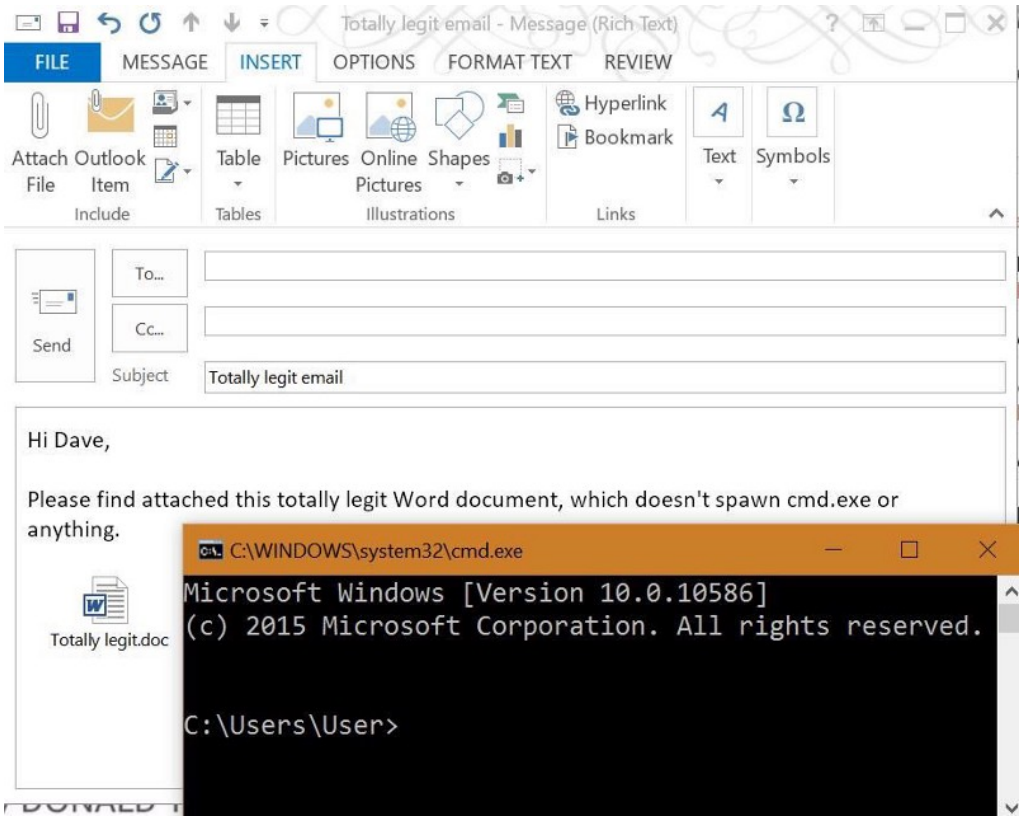
#OLEOutlook - bypass almost every Corporate security control with a point'n'click GUI

In this tutorial, I will show you how to embed an executable into a corporate network via email, behind the firewall(s), disguised as a Word document. There is no patch for this issue.



Earlier this year I wrote about OLE Package, or packager.dll, a Windows feature dating back to Windows 3.1, which still exists in all the latest Windows releases, which allows embedding any content inside documents.

Back then I highlighted you could use this to put malicious content inside Word documents, then swap the format to Rich Text to bypass most Enterprise mail filtering systems.

Next up, Microsoft Outlook.

Yes, Microsoft Outlook from 2003 onwards also supports OLE Packages. By default, Outlook won't allow opening of executable code when received via email as an OLE Package; you simply can't click the icon.

Which is great.

But if you **save the email as a .msg file**, and then attach it to an email, **the user can then open the package.**

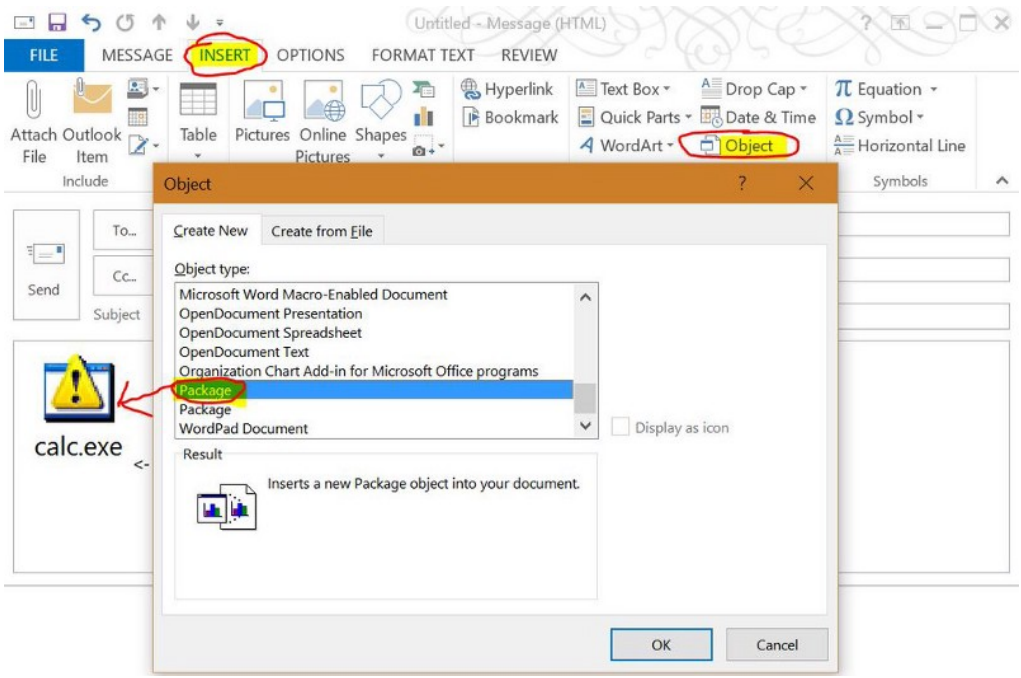
And so far, from all the top Gartner Magic Quadrant mail filtering solutions I've tried, none of them inspect the content *at all*. Test it yourself. You can very likely get all the way to the user desktop, including embedding batch files which antivirus won't flag.

Building the package

What you need:

- Microsoft Outlook 2003 onwards, including Outlook 2016.
- Some hands.

You need to open a new email, maximise the window, then click "Insert" -> Object -> scroll down to Package. Then pick what you want to embed—it might be, for example, Windows Calculator:



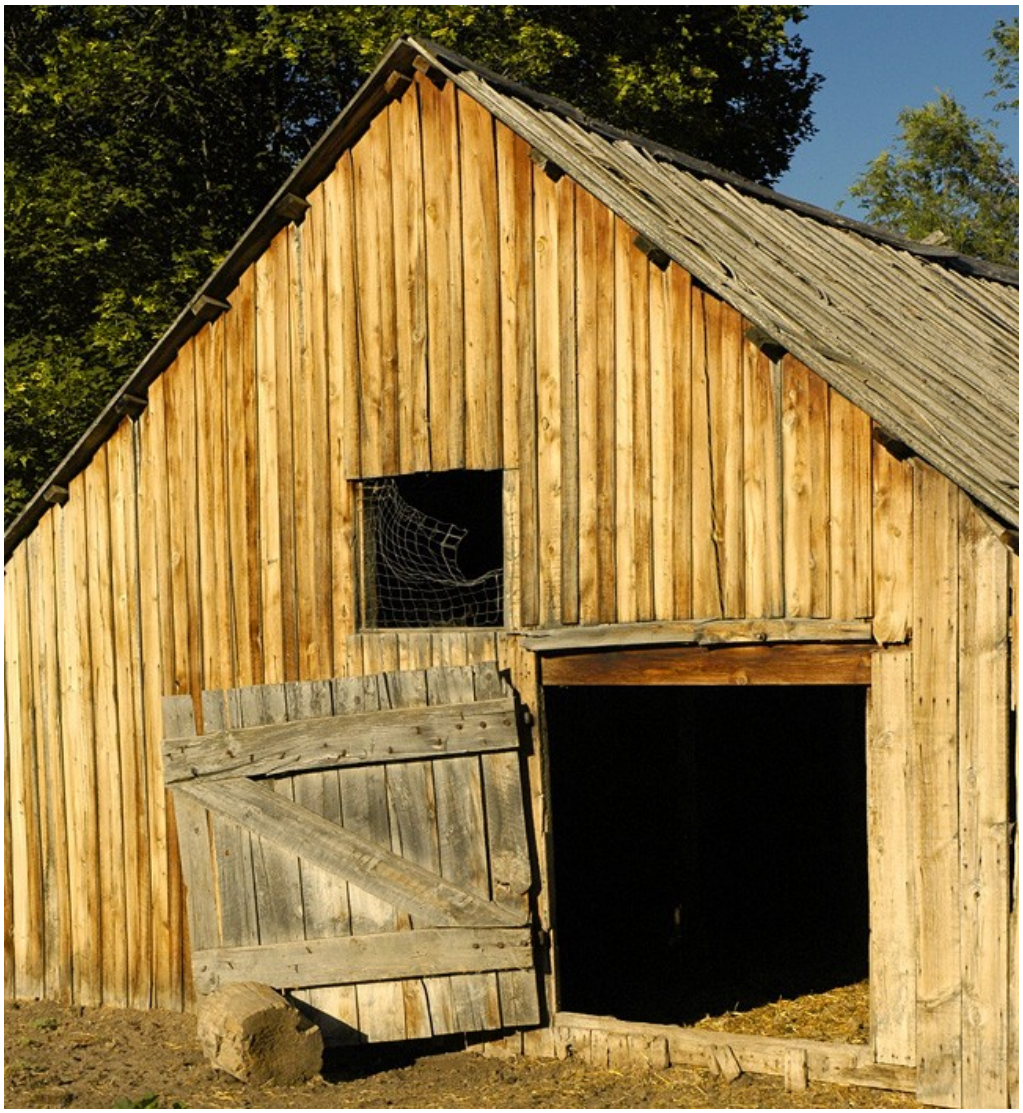
Now click File -> Save As, and give the email a name. E.g. testing.msg.

Then make a new email, tell the user to check the attachment, attach testing.msg, and email it to somebody inside XYZ corp.

The user will get the email. If they open the testing.msg file, then open the executable and okay the prompt, you're in.

"It's okay, our defenses stop this"

They probably don't. For example, Exchange level protector Sophos PureMessage can't apply policy to OLE Packages—so if you filter out .exe files, it just sails past. Outlook itself ignores its own rules around risky file types when they're OLE Packages, and allows opening. The cloud providers I've tried don't apply their policies around .exe files to OLE Packages in .msg files.



To make matters worse, Outlook.exe runs as Medium integrity, and spawns the executable (or batch file, or whatever you embed) as Medium. So you're

out of the Outlook and Windows sandbox, Protected View no more, with a few minutes work.

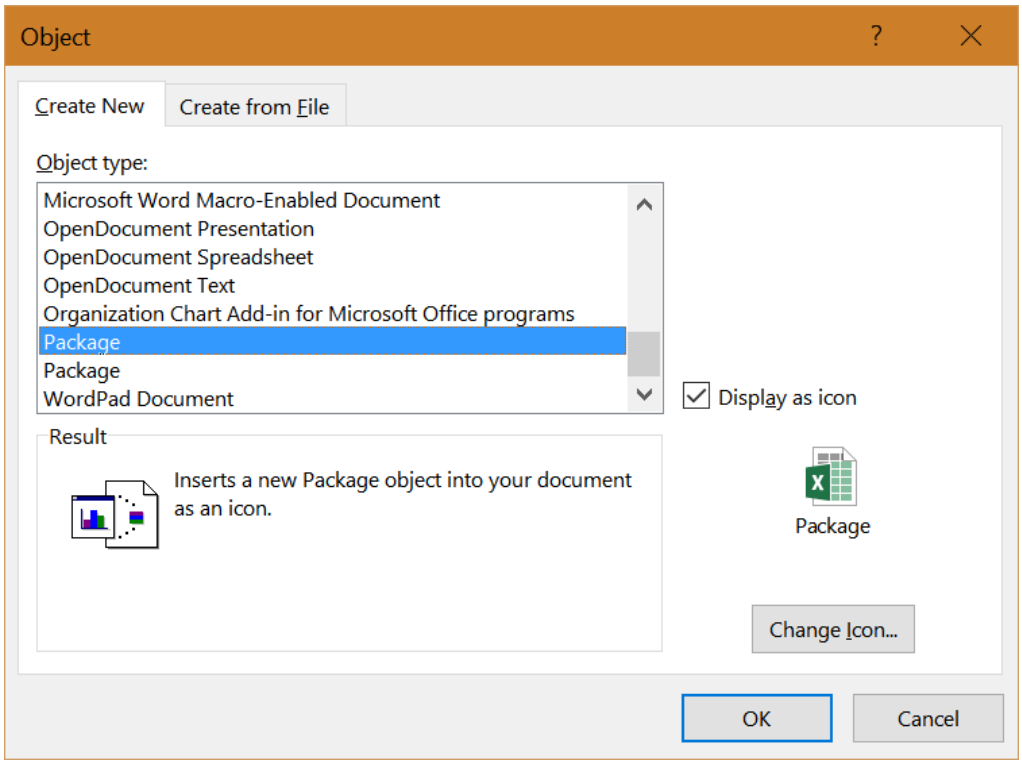
Make me pretty

The next challenge is to replace calc.exe with a warning symbol next to it with something pretty.

You cannot click the "Display as icon" tick box in Outlook, which would allow you to change both the icon and description…

Except in Outlook 2013, you can. Swap the message format from HTML to Rich Text, then return to Insert -> Package.

Ta-da. Tick the "Display as icon" option, then pick a new icon—Winword.exe and Excel.exe are good choices—and in the following screen rename the attachment to, for example, invoice.docx:



Now change the message type back to HTML (important, or the OLE Package is stripped), and save the email.

In the above example, you open Invoice.docx, blindly click through a security warning, and then Firefox Setup kicks in (stealth corporate Firefox rollout confirmed).

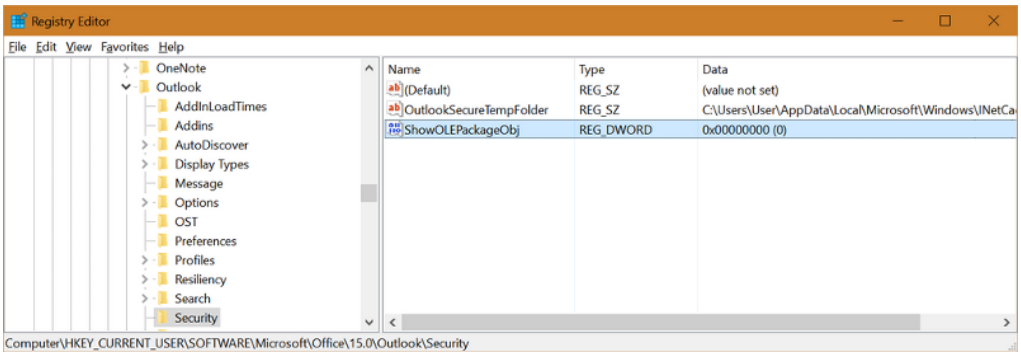
Further

When composing your email, enable the "From" field and make it look like the HR manager sent the email. When the user opens the email, the From field shows the internal HR person.

Protection

Three avenues available:

- Application whitelisting. However, be careful for signed executables with parameters being embedded. E.g. there are many Microsoft digitally signed tools you can use to springboard for other content, and because they're Microsoft you've probably already trusted their publisher certificate.
- Deploy the registry key ShowOLEPackageObj, for your version(s) of Office, to silently disable OLE Package function in Outlook. There is no way to disable it in wider Office, however, so attackers can still embed inside Word, Excel and PowerPoint.



- EMET. If you run Microsoft EMET (or a similar product such as Palo-Alto TRAPS), add this mitigation for Outlook.exe:

```
<Mitigation Name="ASR" Enabled="true">
        <asr_modules>packager.dll</asr_modules>
      </Mitigation>
```

By stopping packager.dll, you stop the issue.

Summary

This is one Microsoft need to tidy up. There is no way a user should be able to click Invoice.docx with a Word icon and spawn unknown code, outside of any sandboxing or control.

FAQ

Is this the same as #BadWinmail (CVE-2015–6172 MS15–131 KB3116111)?

No. That is a different, great, patchable issue found by Haifei.

Do you have a prebuilt test file?

Yes. Check out this document. It just spawns Firefox setup (and is digitally signed by Mozilla). You can attach it to an email and email it your company. There's obviously better ways of demonstrating it, however.