GLASSWALL

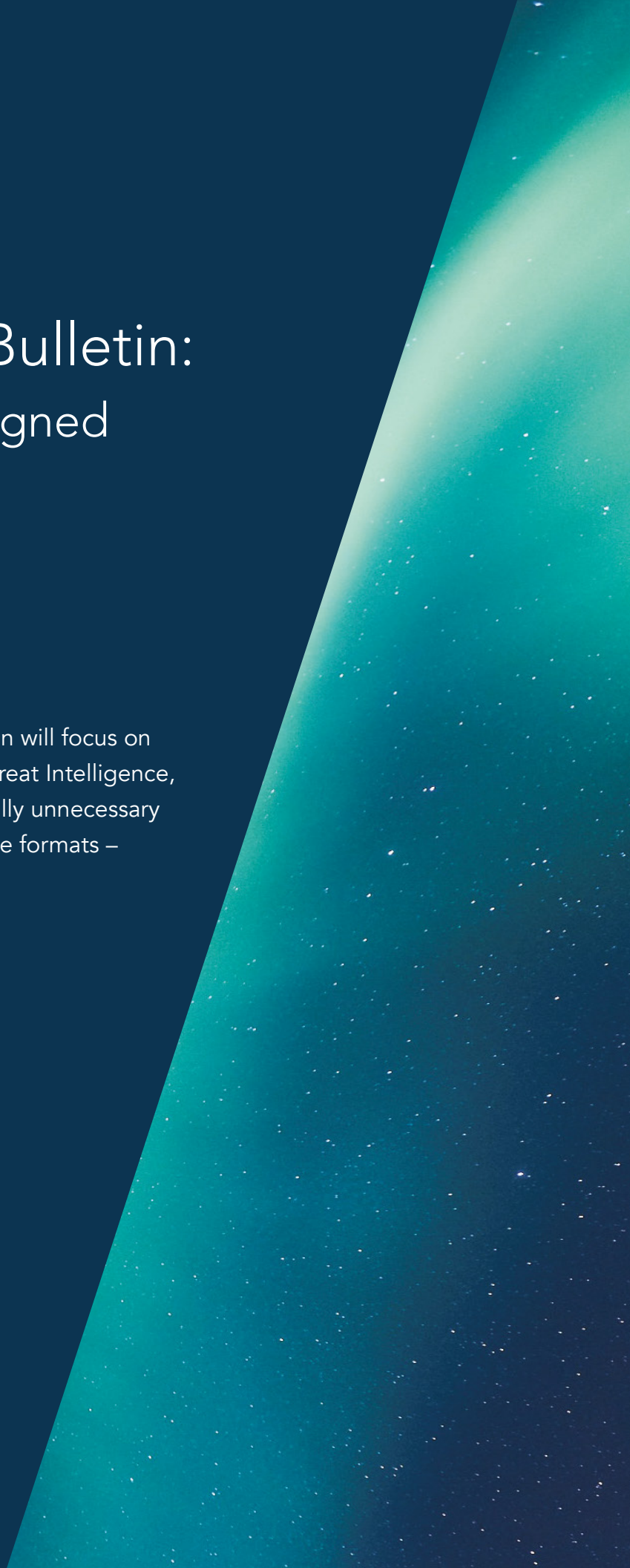
Threat Intelligence Bulletin:

Is Your Business Still Designed for Microsoft XP?

March 2019

By Lewis Henderson

This inaugural Glasswall Threat Intelligence Bulletin will focus on insights from our dynamic Glasswall FileTrust™ Threat Intelligence, enabling us to surface the significant and potentially unnecessary risks organizations face when allowing in legacy file formats – far more common than one might think.



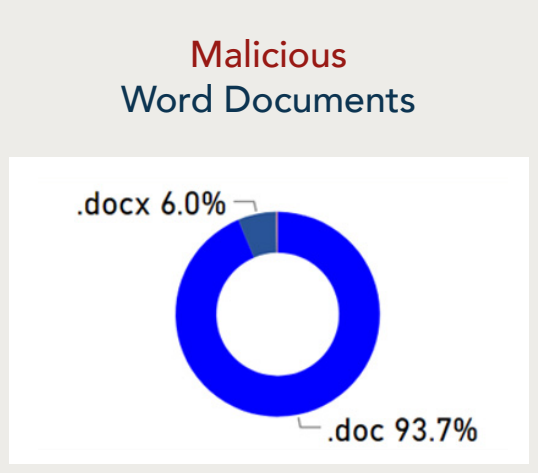
GLASSWALL

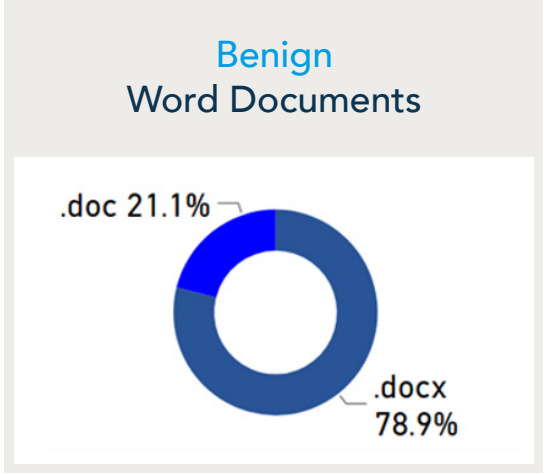
Is Your Business Still Designed for Microsoft XP?

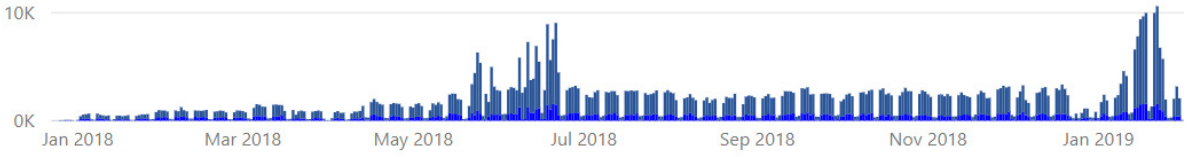
With Windows 7 recently announced as going EOL next year, it gives perspective on how long ago Windows 95 and XP were put to bed. When thinking of Windows XP, does "relic" come to mind, in addition to "insecure"?

If so, consider this: does your organization still allow the use of Microsoft Office® file formats designed for those long-since-retired platforms.

To put that in perspective, below is a chart of the malicious Office Word documents gathered across 2018 from Glasswall's FileTrust™ Threat Intelligence.







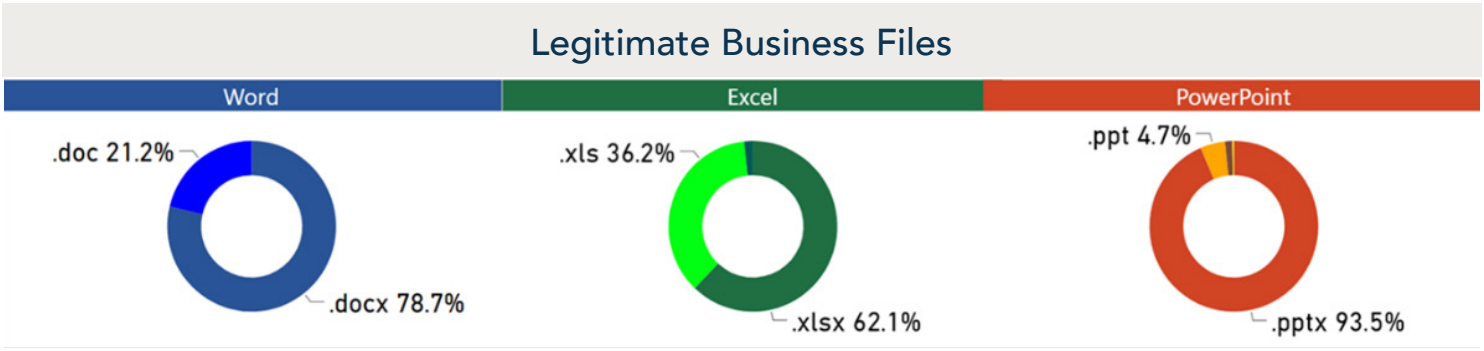
The risks appear to lie in the differences between older and newer file formats. Office binary formats ('97-'03) had only proprietary specifications, no data compression, and function using simple C Data Storage.

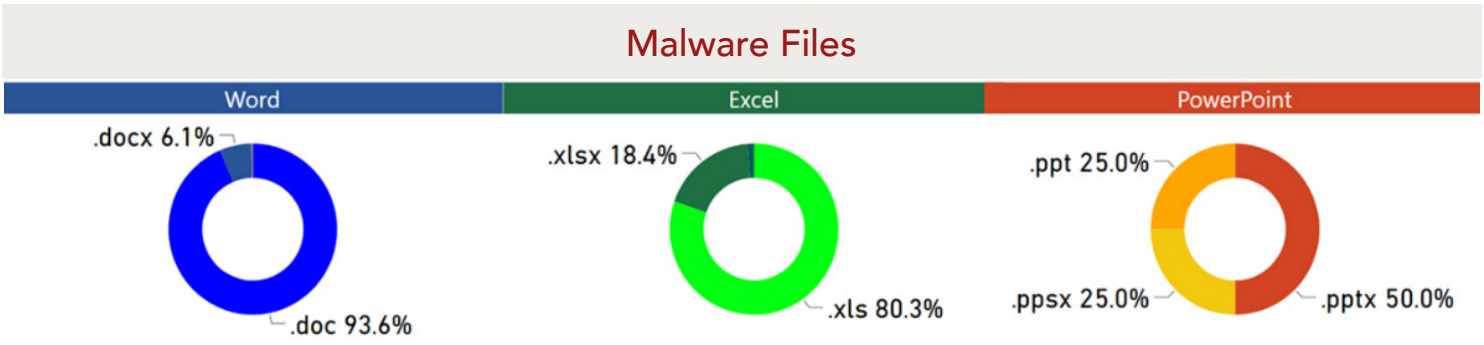
Newer Open Office XML (OOXML) formats ('03 onwards) have a highly defined published file specification, offer lossless compression and have more complex file structures likened to an archive file with multiple subfolders. There are also specific formats for files that optimize Macros more on that later.

The day-to-day advantages of OOXML are pretty obvious, but it seems not everyone has gotten the memo about risks associated with Office Binary files, as we continue using them for some reason.

GLASSWALL

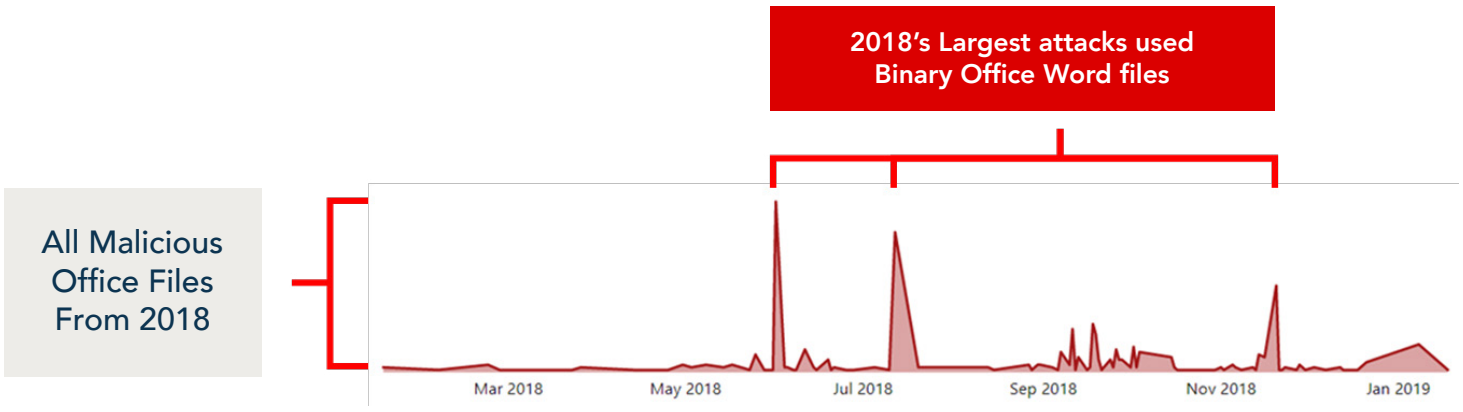
During 2018, these are the comparisons between legitimate and malicious OOXML and Office Binary files. Word is the most extreme. Of all incoming Word documents, 21 percent are older Office binary formats, compared with malicious files, of which 93 percent are Word.





By simply disallowing .doc files, you're wiping out 93% of the malware coming at your organisation in Word documents – food for thought.

Our Threat Intelligence data also clearly shows that older Office files were used in the largest attacks we saw throughout 2018, with Word files in particular being used most often as seen below.



By now many readers are saying "we don't use XP, I haven't seen an Office Binary file for years." Yes, but it may well be that your supply chain still does, they keep sending them and Office will just open all manner of files and formats, making life easy for you.

And what about Macros……..

If I told you 98% of Malicious Office Binary files had Macros, it puts the risks in context, because attackers are choosing that technique over the XML where that figure drops to 0% (except for file types .docm, .xlsm, .pptm that are all exclusively designed to run macros).

You can shut down a major organizational risk just by preventing .doc, .xls and .ppt. Less easy is the path to guide your supply chain, customers and partners down the same route, but move on we must.

Our data clearly show that disallowing legacy file formats will dramatically reduce malware by a huge margin, and where possible disallowing the combination with Macros goes a lot further. It also shows that attackers have found it increasingly more challenging to turn newer OOXML into weapons, and this has to have currency when making potentially seismic shifts in breaking old habits.

These are significant risk reduction numbers that translate to real money saved and real productivity sustained.

UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652
sales@glasswallsolutions.com
glasswallsolutions.com
Glasswall Solutions Limited
@glasswallnews