KnowBe4
Human error. Conquered.

Security Awareness Training Blog

16
Jul

Attacker’s Use of OneDrive as a Malicious File Host Jumps Over 3200% in Q1

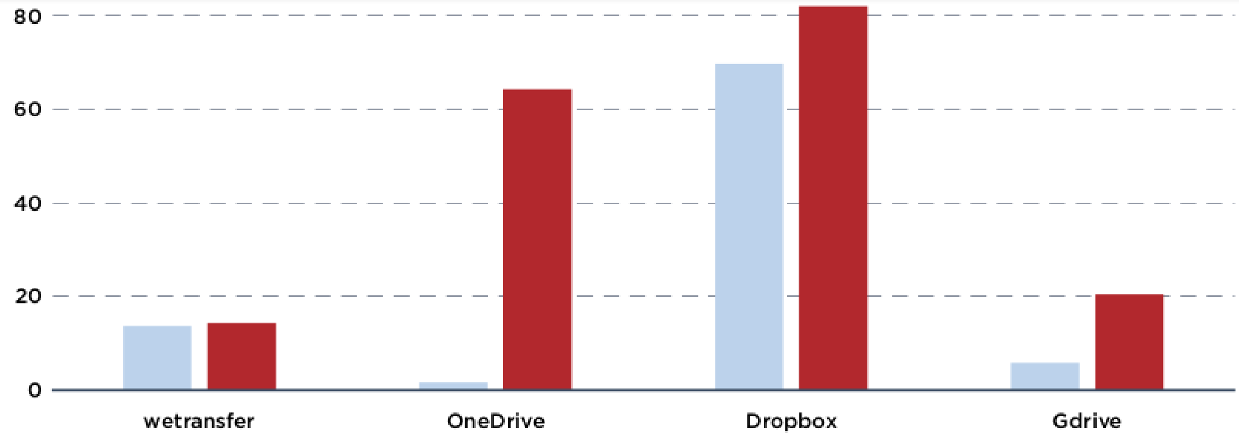
Stu Sjouwerman

Tweet Share Like 31 Share

The need for reputable hosting services to make phishing scams involving malicious files look legitimate has caused a rise in popularity for Microsoft’s cloud-based file sharing service.

According to the Q1 2019 Email Threat Report from security vendor FireEye, an increase in the use of popular cloud hosting services has been seen. Dropbox continues to dominate, having the most detections, but increases are seen for Dropbox, Google Drive *and* OneDrive.

But it’s the massive jump in OneDrive detections (see below) that clearly shows a shift in strategy for some phishing scammers. While the report isn’t entirely clear on the scale of the detections shown below, the numbers on the left are some multiple of the count of detections. In the last quarter of 2018, OneDrive has barely registering (we’re estimating a value of 2 on the chart). But in Q1, the number jumped approximately 32 times that value – a 3200% increase!



This is a much larger concern than being reported elsewhere; misunderstandings of the chart data has some reporting only 60% increases (still a material jump), but the chart isn't displaying percentage of share – it's the number of detections, according to the report.

The use of these well-known sites is due to their ability to get past domain reputation checks, bringing their malicious payloads one step closer to the potential victim.

With OneDrive consistently one of the "big three" file sharing services, it makes sense to take advantage of a user's familiarity of the service as a way to trick them into downloading a malicious file.

Users need to be taught to be vigilant – *especially* when it's a service, company, and even person they are familiar with – so that they don't fall prey to phishing attacks. Organizations that put users through continual Security Awareness Training are best prepared, as their users are aware of the importance of cybersecurity and their role in it, as well as what to look for in phishing attacks – even the ones that look like a harmless file download from OneDrive.