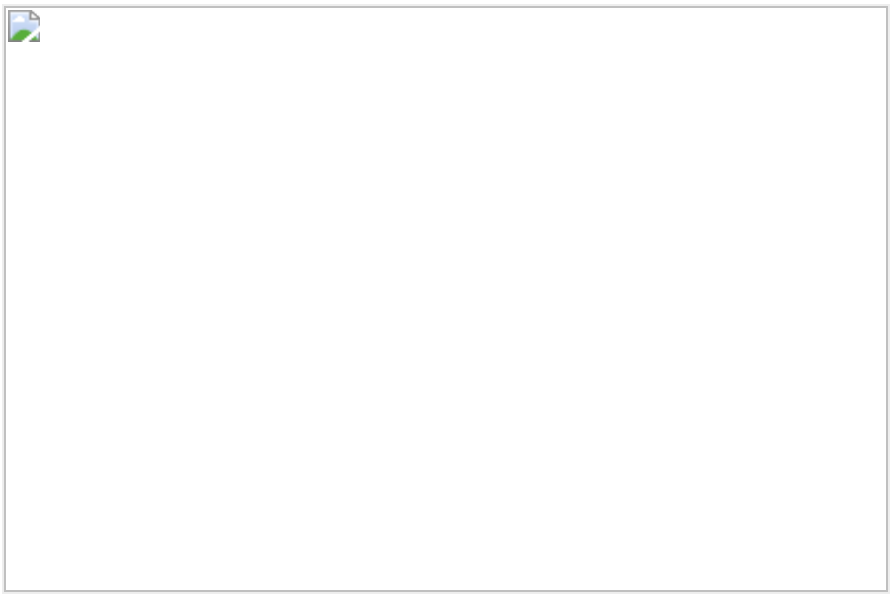
1.5 BILLION secret files found exposed online dwarf Panama Papers leak and expose DNC crimes using Facebook and Google user data

Borked FTP, SMB, rsync, and S3 buckets fingered

By John Leyden 4 Reg comments SHARE ▼



Security researchers have uncovered 1.5 billion business and consumer files exposed online – just a month before the General Data Protection Regulation comes into force.

During the first three months of 2018, threat intel firm Digital Shadows detected 1,550,447,111 publicly available files across open Amazon Simple Storage Service (S3) buckets, rsync, Server Message Block (SMB), File Transfer Protocol (FTP) servers, misconfigured websites, and Network Attached Storage (NAS) drives.

This included documents spanning payroll data, tax returns, medical records, credit cards and intellectual property. A staggering 64,176,425 files came from the UK alone.

The trove amounts to more than 12PB (12,000TB) of exposed data – more than 4,000 times larger than the Panama Papers leak, which weighed in at a measly 2.6TB.

The most common data exposed was payroll and tax return files, which accounted for 700,000 and 60,000 files respectively. However, consumers were also at risk from 14,687 instances of leaked contact information and 4,548 patient lists. A large volume of point-of-sale terminal data – transactions, times, places, and even some credit card details – was publicly available.

Although misconfigured Amazon S3 buckets have hogged headlines recently, in this study (registration required) cloud system leaks accounted for only 7 per cent of exposed data. Instead it is older, yet still widely used, technologies – such as SMB (33 per cent), rsync (28 per cent) and FTP (26 per cent) – which have contributed the most.

Business-critical information also leaked. For example, a patent summary for renewable energy in a document marked as "strictly confidential" was discovered. Another case included a document containing proprietary source code submitted as part of a copyright application. This file included the code that outlined the design and workflow of a site providing software Electronic Medical Records, as well as details about the copyright application.

Third parties and contractors were identified as one of the most common sources of sensitive data exposure. The leaked information included security assessment and penetration tests. In addition, Digital Shadows identified consumer backup devices that were misconfigured to be internet-facing and inadvertently making private information public. ®

It's much worse: Facebook says almost every profile has had its data scraped by a third party (cnbc.com)

by Frank_Castle to **news** (**+17** | **-0**)

1 comment


It's