Researchers recover 75,000 'deleted' files from pre-owned USB drives

November 4 2020

Professor Karen Renaud. Credit: University of Abertay Dundee

Highly sensitive tax returns, contracts and bank statements were among 75,000 "deleted" files recovered by cybersecurity researchers as part of an Abertay University investigation into the risks of selling used USB

drives over the internet.

The team, from Abertay University, made the startling discovery after purchasing just 100 devices on a popular online auction site and examining them further.

98 of the USBs seemed, at face value, to be empty. However, with publicly available tools it is worryingly easy to retrieve data.

Only 32 of the drives had been properly wiped. Partial files were extracted from 26 devices and every single file was extracted from the remaining 42 USB drives.

Many of the files extracted were determined to be of high sensitivity, and included files named "passwords", contracts, bank statements and tax returns.

Other USB drives contained images with embedded location data.

Professor Karen Renaud from Abertay's Division of Cybersecurity, said: "This is extremely concerning, and the potential for this information to be misused with extremely serious consequences is enormous. An unscrupulous buyer could feasibly use recovered files to access sellers' accounts if the passwords are still valid, or even try the passwords on the person's other accounts given that password re-use is so widespread. They would likely be able to find a seller's e-mail address from the files we found on the drive. They could try to siphon money from the bank accounts or even blackmail a seller by threatening to reveal embarrassing information."

Professor Renaud said that the sellers would not have been aware that they had left data on the drive: "A lot of people don't realize it, but the way many computers delete files doesn't actually remove them. What

happens is that the file is removed from the index so that they are effectively hidden from view. They're still there though and if you know how, you can easily recover them using publicly available forensics tools. Software is freely available that can permanently wipe USB drives, so if you are going to sell a device we would strongly recommend using that. If you're planning to discard a USB device without selling it, you should destroy it with a hammer—make it impossible for a third party to get hold of the data it stores. If you're planning to buy a new USB drive, the best way of mitigating the risks is to buy an encrypted device."

Interestingly, none of the drives held any viruses or other malware, which meant that a buyer would be perfectly safe using the purchased drives.

The research, led by student James Conacher for his Masters project, found that while the risks to the sellers were high, buyers faced no risks for these specific 100 drives.

More information: James Conacher et al. Caveat Venditor, Used USB Drive Owner, *SSRN Electronic Journal* (2020). DOI: 10.2139/ssrn.3631441

Provided by University of Abertay Dundee