Forensic finder exploring Windows calls attention to mail pile

September 24 2018, by Nancy Owano

Credit: CC0 Public Domain

Is Windows storing your email? Not the most comforting thought, as we recover from the Facebook user data headlines earlier this year. Nonetheless, storing of email grabbed the attention of Joel Hruska,

ExtremeTech, and other tech watchers recently when they learned of a disturbing discovery by Jeremy Skeggs.

Skeggs, a forensic analyst, considered a Windows 8.1 and 10 design decision worthy of a closer look. Skeggs stated outright on GitHub: "'WaitList.dat' (WaitList) is data file which has been found to contain stripped text from email, contact and document files as a function of the Windows Search Indexer."

ZDNet reported another issue regarding Windows and mail. "A little-known Windows feature will create a file that stores text extracted from all the emails and plaintext files found on your PC, which sometimes may reveal passwords or private conversations."

Long and short, the WaitList.dat file "can be copied in under a second and will likely contain sensitive information or passwords on many people's computers," said Isaiah Mayersen in *TechSpot*.

OK, first concerning Windows 8.1: "I identified the 'WaitList.dat' artefact while investigating a Windows 8.1 PC for the presence of a known email. I was provided with a copy of this email, and part of the investigation involved identifying whether or not this email ever existed on the custodian's computer. After processing the .PST and .OST mailbox archives on the PC, I did not identify the existence of the email. I then processed shadow copies, carved and processed for various mailbox stores and email files, and still did not identify the email. As a final attempt, I ran a string search for the email subject line across the whole forensic image. I received 1 hit within 'WaitList.dat'. Investigation of this 140 mb file identified metadata, and full body text of over 36,000 emails and documents, spanning back three years."

Hruska highlighted a key point that "data stored within WaitList.dat isn't deleted when documents are removed," and it could in turn be used to

recover information from a PC.

If users worry that this file is too much of a hornet's nest, they can eradicate it. Cimpanu at ZDNet said that for those who are concerned about their data, "all you need to do is delete the WaitList.dat file and disable handwriting recognition. "

Cimpanu said at the time of his writing that there was no evidence that data was being uploaded to Microsoft, nor any malware. At the same time, he said, "it would be nice to see Microsoft release an update that stored the file a little more securely."

Latesthackingnews.com, looking at Windows Handwriting Recognition, said "Many Windows users who prefer touch-screen or stylus as input methods know the importance of this feature."

Skeggs wrote that "Since the release of Windows 8 and the 'Metro' interface, touchscreen input has been implemented in a rapidly rising number of Windows devices, including Microsoft Surface Pro/Book, two-in-ones, convertible laptops and tablets. Microsoft has catered for this trend, implementing conversion between touch/pen handwriting to computer text in software such as OneNote."

More information: b2dfir.blogspot.com/2016/10/to … xicon-forensics.html