Microsoft is scanning the inside of password-protected zip files for malware

reader comments

82 with

Microsoft cloud services are scanning for malware by peeking inside users’ zip files, even when they’re protected by a password, several users reported on Mastodon on Monday.

Compressing file contents into archived zip files has long been a tactic threat actors use to conceal malware spreading through email or downloads. Eventually, some threat actors adapted by protecting their malicious zip files with a password the end user must type when converting the file back to its original form. Microsoft is one-upping this move by attempting to bypass password protection in zip files and, when successful, scanning them for malicious code.

While analysis of password-protected in Microsoft cloud environments is well-known to some people, it came as a surprise to Andrew Brandt. The security researcher has long archived malware inside password-protected zip files before exchanging them with other researchers through SharePoint. On Monday, he took to Mastodon to report that the Microsoft collaboration tool had recently flagged a zip file, which had been protected with the password “infected.”

“While I totally understand doing this for anyone other than a malware analyst, this kind of nosy, get-inside-your-business

way of handling this is going to become a big problem for people like me who need to send their colleagues malware samples," Brandt wrote. "The available space to do this just keeps shrinking and it will impact the ability of malware researchers to do their jobs."

Fellow researcher Kevin Beaumont joined the discussion to say that Microsoft has multiple methods for scanning the contents of password-protected zip files and uses them not just on files stored in SharePoint but all its 365 cloud services. One way is to extract any possible passwords from the bodies of email or the name of the file itself. Another is by testing the file to see if it's protected with one of the passwords contained in a list.

Advertisement
"If you mail yourself something and type something like 'ZIP password is Soph0s', ZIP up EICAR and ZIP password it with Soph0s, it'll find (the) password, extract and find (and feed MS detection)," he wrote.

Brandt said that last year Microsoft's OneDrive started backing up malicious files he had stored in one of his Windows folders after creating an exception (i.e., allow listing) in his endpoint security tools. He later discovered that once the files made their way to OneDrive, they were wiped off of his laptop hard drive and detected as malware in his OneDrive account.

"I lost the whole bunch," he said.

Brandt then started archiving malicious files in zip files protected with the password "infected." Up until last week, he said, SharePoint didn't flag the files. Now they are.

Microsoft representatives acknowledged receipt of an email asking about the practices of bypassing password protection of files stored in its cloud services. The company didn't follow up with an answer.

A Google representative said the company doesn’t scan password-protected zip files, though Gmail does flag them when users receive such a file. My work account managed by Google Workspace also prevented me from sending a password-protected zip.

The practice illustrates the fine line online services often walk when attempting to protect end users from common threats while also respecting privacy. As Brandt notes, actively cracking a password-protected zip file feels invasive. At the same time, this practice almost surely has prevented large numbers of users from falling prey to social engineering attacks attempting to infect their computers.

One other thing readers should remember: password-protected zip files provide minimal assurance that content inside the archives can’t be read. As Beaumont noted, ZipCrypto, the default means for encrypting zip files in Windows, is trivial to override. A more dependable way is to use an AES-256 encryptor built into many archive programs when creating 7z files.

https://arstechnica.com/?p=1939441