

Forum:[Hack Forums](#)

Thread: [Zip file encryption an cloud scanners. And can ISO be encrypted?](#)

midichlorianchip - January 15, 2024, 5:18 pm

Hello. I'm doing some experimenting on my local machine. When I read APT campaigns, I realize that their attack vectors normally use a container or archive file (ISO/IMG or Zip) To deliver their payload via email and in some cases cloud services. But how do they pass email scanners?

For example, the .lnk + ISO is a common exploit I see in the wild. Threat actors put shortcut file in ISO/Zip and deliver. But won't scanners pick up the combination of ISO + .lnk and Heuristics should detect it as suspicious?

The general consensus seems to be, password protected Zip files seem to work the best against cloud scanners. Here are my questions.

1. Does password protecting a zip file also prevents the cloud scanners from recognizing mime types?
2. Do the scanners "know" you have a shortcut file within the archive, but just can't scan it for viruses?
3. Do passwords on zip files guarantee that no cloud scanners can scan the files for malicious code?

Thanks

DramaKing - January 15, 2024, 8:01 pm

(Jan 15, 2024 06:18 PM)midichlorianchip Wrote: [\[CITE\]](#) Hello. I'm doing some experimenting on my local machine. When I read APT campaigns, I realize that their attack vectors normally use a container or archive file (ISO/IMG or Zip) To deliver their payload via email and in some cases cloud services. But how do they pass email scanners?

For example, the .lnk + ISO is a common exploit I see in the wild. Threat actors put shortcut file in ISO/Zip and deliver. But won't scanners pick up the combination of ISO + .lnk and Heuristics should detect it as suspicious?

The general consensus seems to be, password protected Zip files seem to work the best against cloud scanners. Here are my questions.

1. Does password protecting a zip file also prevents the cloud scanners from recognizing mime types?
2. Do the scanners "know" you have a shortcut file within the archive, but just can't scan it for viruses?

3. Do passwords on zip files guarantee that no cloud scanners can scan the files for malicious code?

Thanks

File names in archive files can be encrypted. That should take care of any scanning for file types. Bypassing AV after archive is unpacked will still be an issue as will the fact that password-protected zip files are such a common delivery mechanism.