

Forum: [Hack Forums](#)

Thread: [Google Chrome Safe Browsing and ISO, Zip and HTML smuggling.](#)

midichlorianchip - January 20, 2024, 6:39 am

Hey guys and gals. I've been reading APT campaigns written by security companies. I've noticed that the first stage of an attack basically is always one of:

Email + ISO
Email + password protected zip
Email + ISO

So I decided to do some testing. My goal was to see how Google's Safe Browsing, on highest settings can affect hacking. I've noticed some behavior that I want clarification on. How does Google Chrome and Safe Browsing approach archive files? I've read Google's documentation, but I want practical feedback.

1. Does Safe Browsing block certain file combination on sight? Archive in Archive or Password Protected archive in non-password protected archive.
2. Does Safe Browsing extract Archive and scans each file within the archive?
3. Does Safe Browsing blocks certain archives once they detect certain file types within archive? (.lnk, .exe, .vbs, .ps, etc.?)
4. What role does crypting payloads play in bypassing Safe Browsing
5. Does using HTML smuggling (using JavaScript Blobs) to download archives give protection from Safe Browsing vs downloading archive normally?
6. Does password protecting archive guarantees protection from Safe Browsing?
7. How do APTs by pass Safe Browsing using ISO? Safe Browsing should be able to extract or scan inside ISO.

Thanks

Nemo5 - January 21, 2024, 11:09 am

1) Yes, it block nested archives or password-protected archives.

2. Yes.

3. If they contain files with known malicious types, such as .lnk, .exe, .vbs, or .ps, yes.

4. It may enhance evasion, as it could make it challenging for Safe Browsing to identify malicious patterns.

5. It might provide a degree of protection.

6. No.

7. APTs might exploit vulnerabilities or employ sophisticated techniques to bypass Safe Browsing when using ISO files. This could involve evading detection during extraction or utilizing specific encryption methods.

Ph4n70M Phr34K - January 29, 2024, 5:52 pm

This thread might be interesting for you: <https://hackforums.net/showthread.php?tid=6244776>