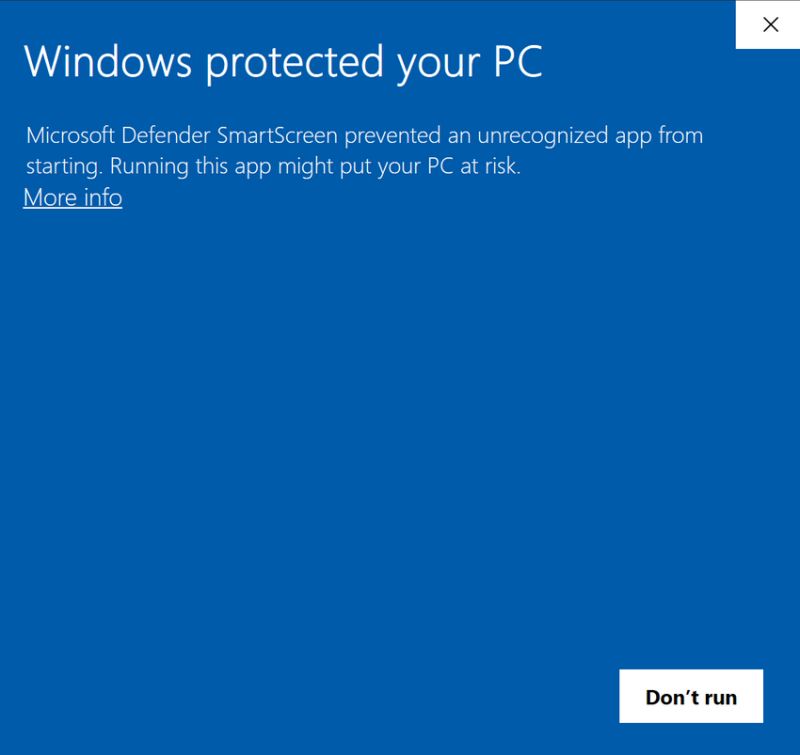
**Red Team exercise**

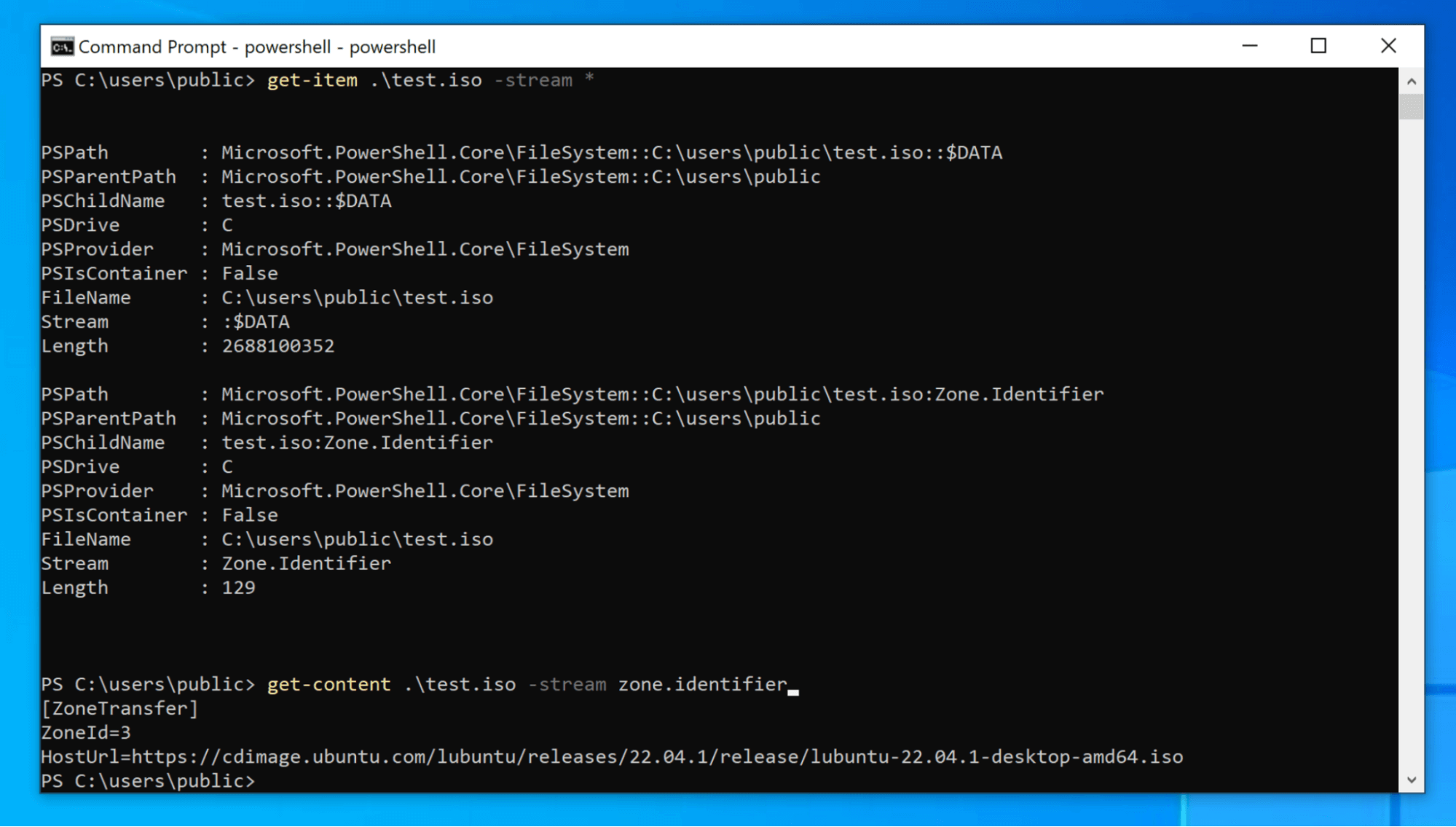
1. **SmartScreen Bypass and Mark-of-the-Web**

During red team exercises in infrastructures with Windows 10 or 11 machines, your malicious artifact may be blocked by the smartscreen.

Smartscreen About:  
  
SmartScreen is a Microsoft security technology designed to protect users against web threats such as malicious websites, unsafe downloads, and phishing. Originally introduced as part of Internet Explorer, SmartScreen is now integrated into Microsoft Edge and Windows 10 and 11.



This hidden tag tells Windows (and apps like Office, PowerShell, or SmartScreen):  
 “**This file came from the web. Treat it with caution.**”

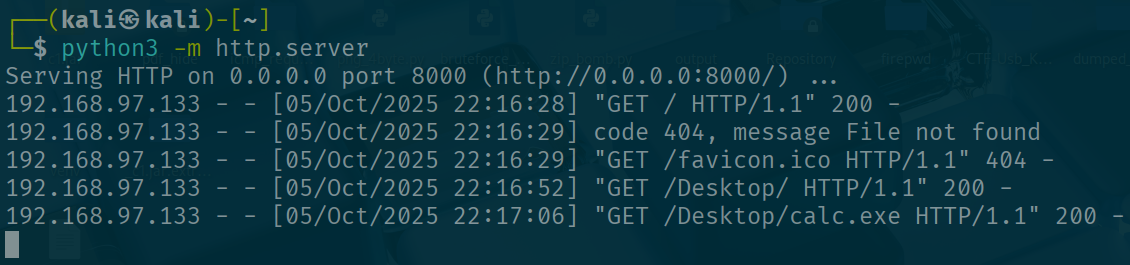


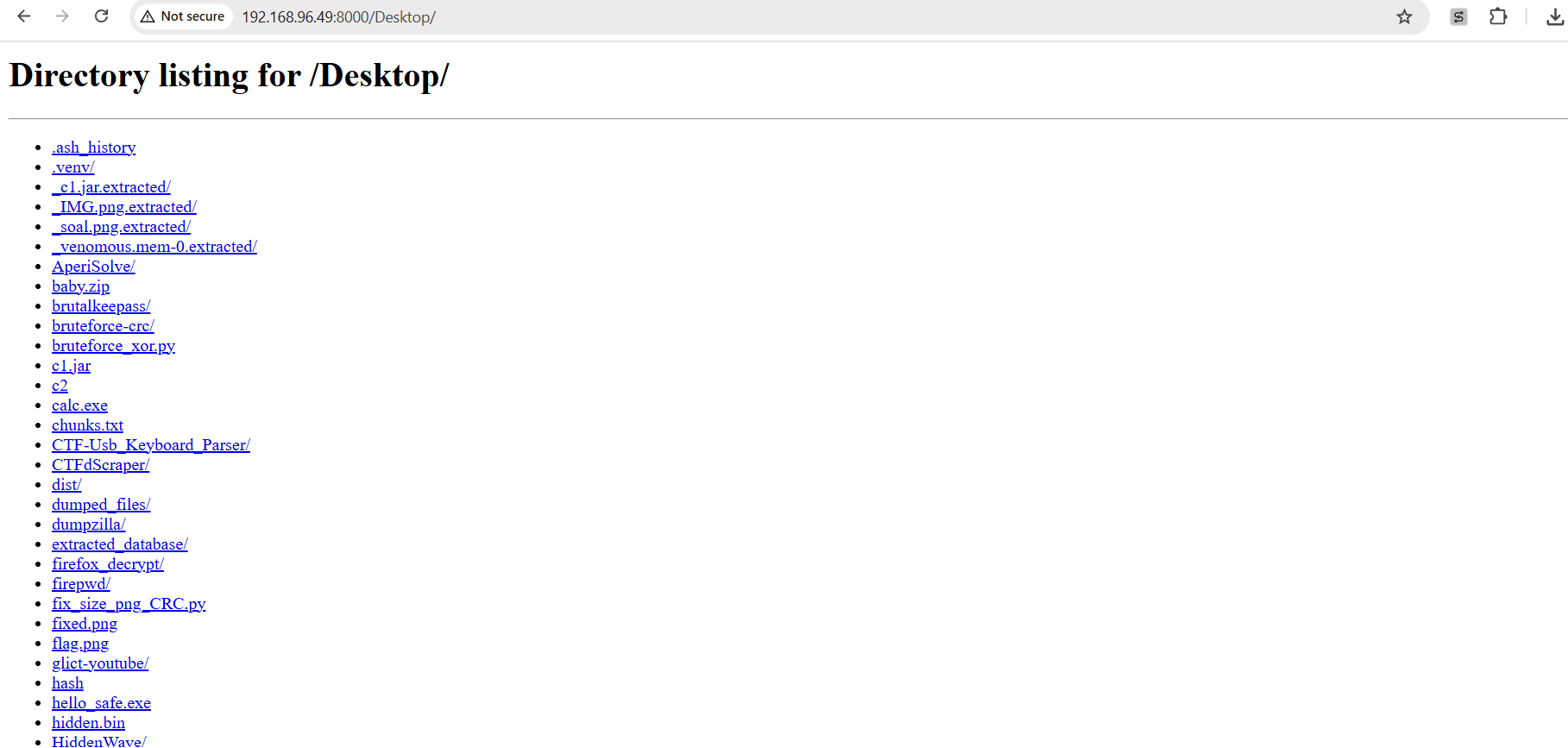
* 1. **Scenario**

For example, when you download a .docx or .exe from your browser or email, it gets a MOTW tag like this:

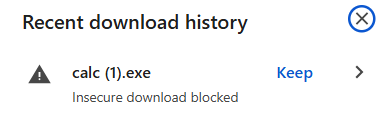
[ZoneTransfer]  
ZoneId=3

* ZoneId=3 means *Internet Zone*.
* Other values include 0 (My Computer), 1 (Local Intranet), 2 (Trusted Sites), and 4 (Restricted Sites).
  1. **Bypass Mark-of-the-Web**
* **Attacker**

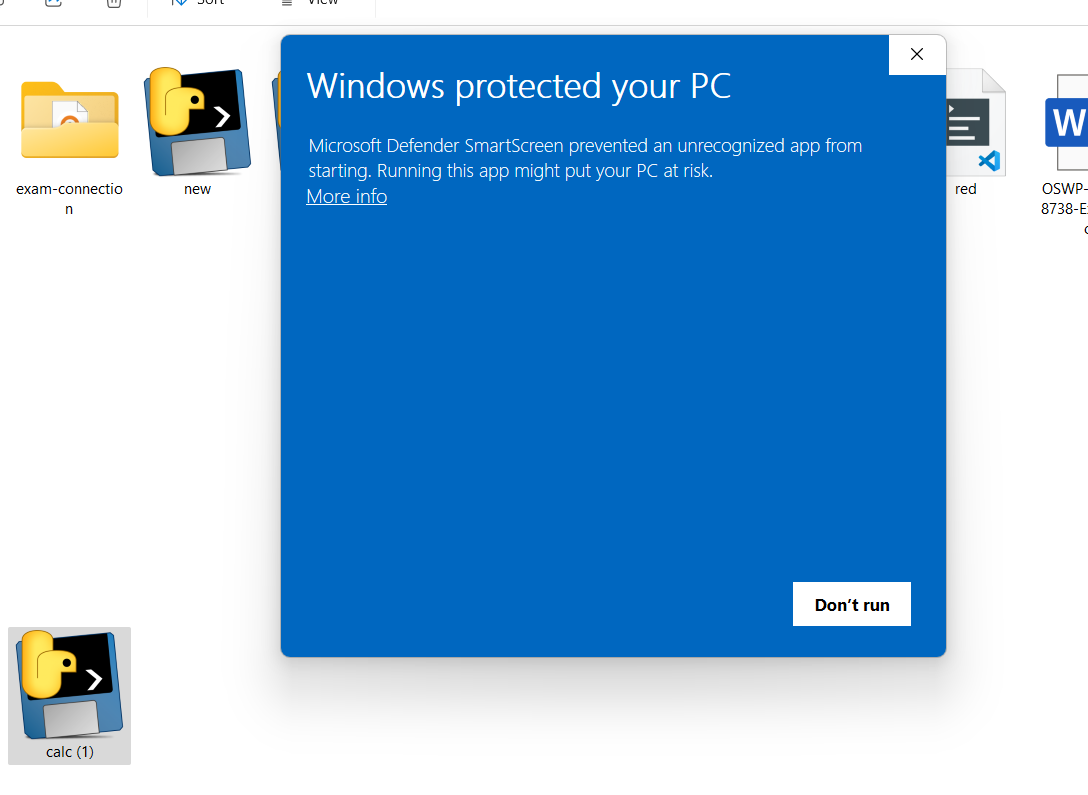
****

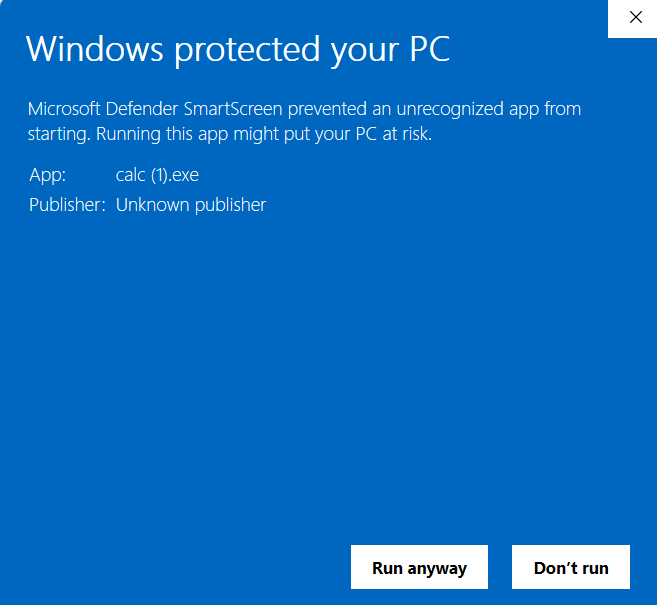
****

Attacker download it directly and it shows it is insecure download blocked Then attacker clicks Keep

****

When malicious user clicks exe it will prompt smart screen

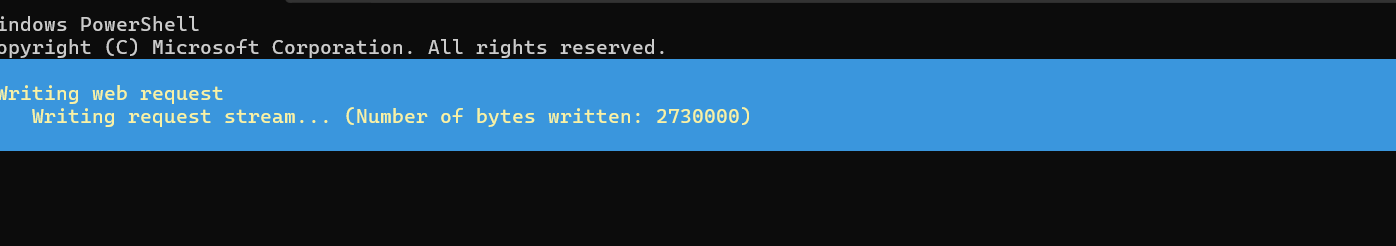
****

****

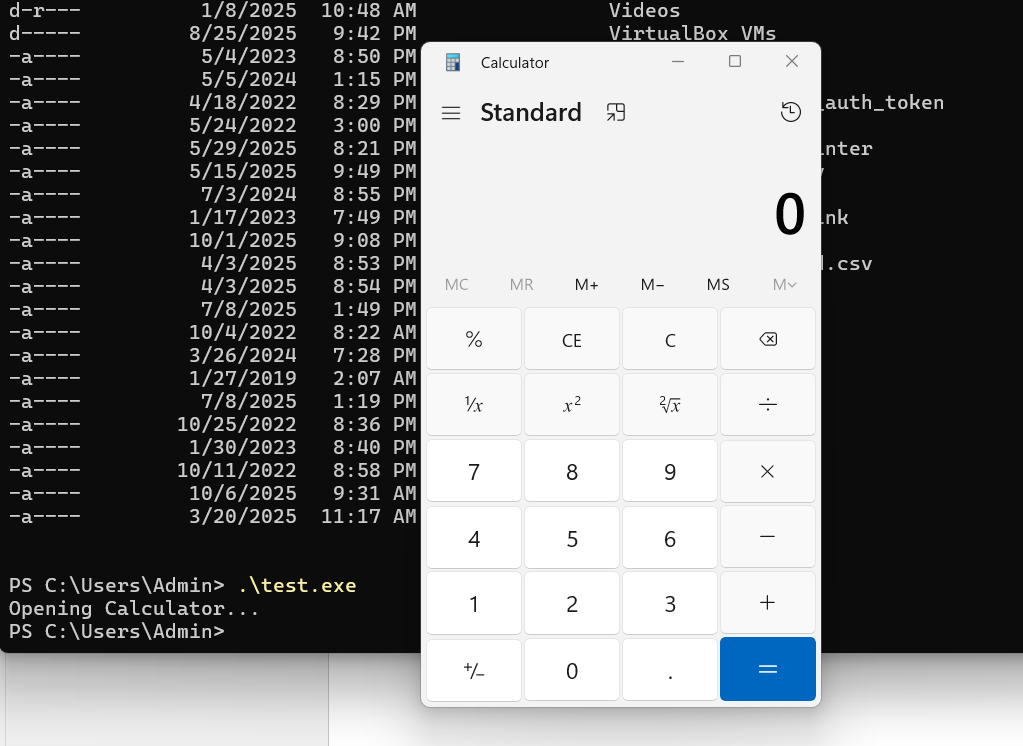
and sometimes if windows defender detects malicious activities it will delete it

**To bypass smart screen**

****

****

It doesn’t alert smart screen or Mark of the Web

****

Reference: <https://redcanary.com/threat-detection-report/techniques/mark-of-the-> web-bypass/