

# APT Attack Simulation 29

Date:5/17/2023



# Authors

---

Abdallah Mohammed

[Github](#)

---

Abdulrahman Mohammed (De3vil)

[Github](#)

---

Hossam Ehab (0xHossam)

[Github](#)

---

# Documentation

- How does the attack work?





# First stage

- The attack begins with an email that contains a specially crafted HTML page that includes a malicious code. Upon opening the malicious page, an ISO file is downloaded that contains the malicious files.
  - The malicious file performs two actions
    - 1- Drops an ISO file (Second Stage)
    - 2- Sends a request to a malicious SMB server controlled by the attackers to steal the user's NTLM Hash for lateral spread.



## Second stage

- The ISO file is opened and contains a forged Ink file that appears to be a PDF file from its icon, but it actually points to an exe file. When the exe file is executed, it opens the PDF file.
- Upon execution of the malicious exe file, the PDF file is also executed. DLL and bin files are loaded, a registry key is added for persistence, and the DLL runs  
During this stage.
- At this point, the attacker enables UAC bypass, gains system administrator privileges, hijack Windows Defender, and loads the malicious DLL instead of the original file. This allows the attacker to invisibly direct the malicious functions on the victim's machine, download more malware, and achieve system persistence.

## Third stage

- The DLL acts as a Loader to read the encrypted bin file and decrypt it in memory and try to hide from detection and run.