

AV Bypass

@hack-stuff.com

What's AV ???



卡提諾 CK101.COM

It's Antivirus



ESET Smart Security 5
病毒防護 | 反間諜軟體 | 防火牆 | 反垃圾郵件

第5代 ESET Smart Security 是一套綜合性安全套件，集反病毒，反間諜、個人防火牆和反垃圾郵件於一身。同時集成一系列增強型安全功能。

[了解更多 ...](#)

[立即購買 ▶](#) [下載試用版 ▶](#)

An image of the ESET Smart Security 5 software box, which is white with a yellow vertical bar on the left containing the product name and a portrait of a person in the center.



The Trend Micro logo consists of a red circular icon with a white 't' shape inside, followed by the word 'TREND' in a bold, black, sans-serif font, with 'MICRO' in smaller letters below it.

Securing Your Journey
to the Cloud

學習免殺必備的知識

- 簡單的ASM
- PE文件格式
- OD 等工具使用

防毒軟體有哪些招式!!

- 特徵碼比對
- 啟發式
- Sandbox 虛擬技術
- 脫殼
- 主動防禦
- MD5比對

常見Bypass方法

	特徵碼免殺	無特徵碼免殺	源碼免殺
持久度	最差	中等	最好
難易度	簡單	較難	中等
成效/時間	低	中	超高高高高
過防毒數量	單一	多個	多個
總結	淘汰	堪用	猛!!!!

特徵碼免殺

- 利用工具定位出特徵碼
- 等價替換



無特徵碼免殺

- XOR加密
- 隱藏輸入表
- 改殼
- 時間延遲
- 反啟發應用

源碼免殺

- 主要利用編譯器選項
- 區段合併
- 體積優化
- 添加反虛擬機、反調適代碼

創新與突破

- 參考別人的作品，從中提取實用的代碼
- 找尋實體與虛擬機的差異，利用比較進行突破

Thanks ;)