

A Real Attack - Nim material



by @SayantanHack

What all are Real Attacks ?

- All attacks are real
- It depends on the perspective and the impact (Risk Factor)
- Except Movies



Exploitation : {using : "Malware"}

- Platform : "Windows"
- Arch : "x86 | x64"
- Method : "DLL Injection | Shell Code Injection"
- Tools : { Lang : "Nim" ,

Lib: "Winim"

}

Nim ??

- Nim is a statically typed compiled systems programming language
- Performance : C ;
- Syntactically : Python;
- Translate to C then compiled

<https://nim-lang.org/>



Detectability ??

- Off course **Yes**.
- This no means can be 100% EDR/ AV/ Defender proof
- Just a POC
- If you can hide in a Haystack Go ahead....

How to H4ck

- Git clone the nim code [https://github.com/sayantanHack/thm_maldev/]
- Create a Shellcode [<https://github.com/BishopFox/sliver/wiki>]
- Generate a session on sliver
- Transfer the payload to victim
- Exploit

L3t's H4ck

