Has this file been identified as malicious? Explain why or why not.

IDS detects a user downloading a file that is not trusted, the hash looked up is deemed by virustotal to be an executable malware/trojan/backdoor software deemed by almost every vendor. Deeming the file as malicious.

The Pyramid of Pain

Level	Difficulty
TTPs	tough
Tools	challenging
Network/host artifacts	annoying
Domain names	simple
IP addresses	easy
Hash values	Trivial ←