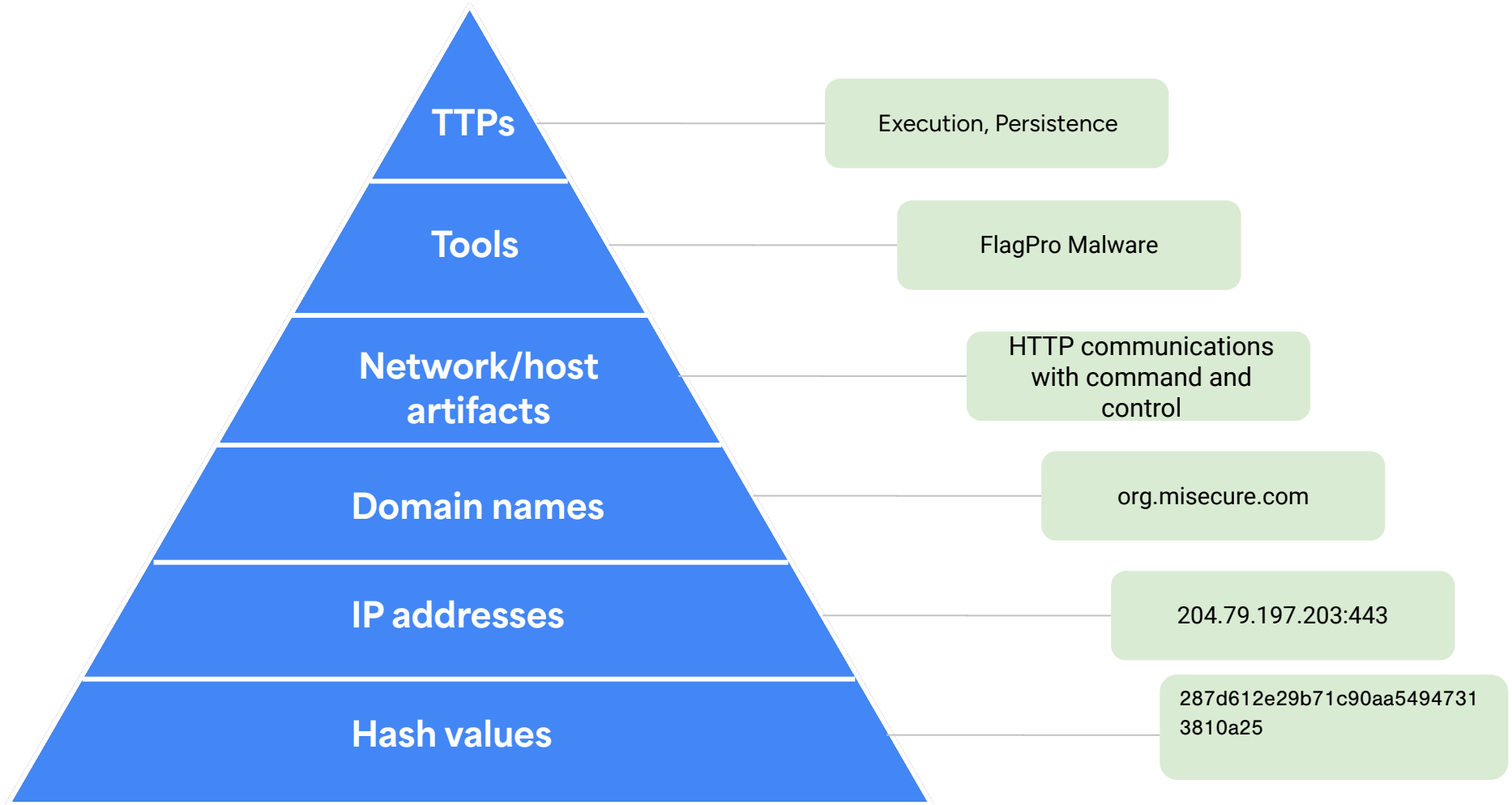
Project,

On Wednesday, January 15, 2025, at 9 AM EST, I received an alert regarding a suspicious file download on an employee's computer. Upon investigating the alert, I discovered that the employee had received an email containing a password-protected spreadsheet attachment, with the password provided in the email. After downloading and opening the file using this password, a malicious payload was executed on the employee's machine.
To address this incident, I retrieved the malicious file and generated a SHA256 hash to uniquely identify it. This hashing process acts as a digital fingerprint that cannot be decrypted, which is crucial for tracking and managing malware threats effectively. Following this, I input the hash into VirusTotal to gather more information about the file and assess its potential risks.

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

This is a malicious file reported by 58 vendors with a community score of -229. The popular threat label is trojan.flagpro/fragtor. Flagged as a virus by 3 different sandboxes. The behavior tags are typical of malicious software, particularly the "self-delete" and "persistence" tags.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Execution, Persistence
FlagPro Malware
HTTP communications with command and control
org.misecure.com
204.79.197.203:443
287d612e29b71c90aa5494731 3810a25