

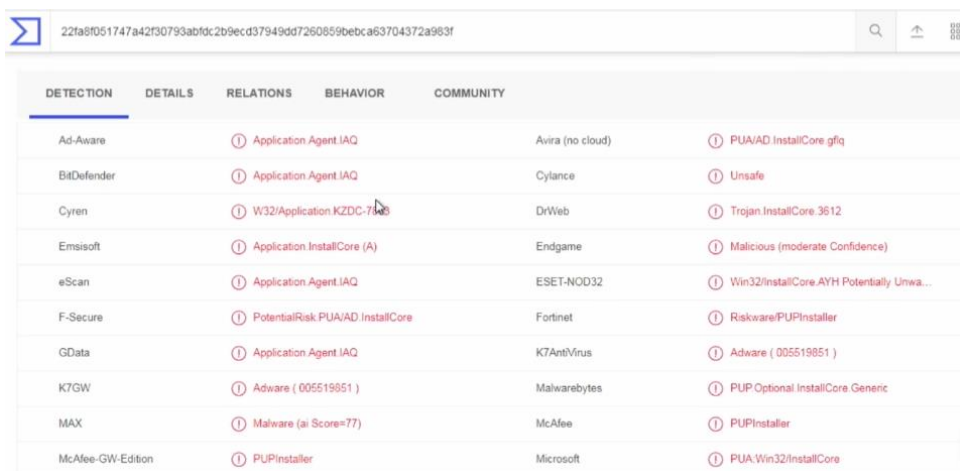
Curso Análisis de Malware

Los pasos para analizar un malware son retención, contención, identificación, comparación, extracción, análisis estático, análisis dinámico y realizar un informe.

El análisis estático consiste en estudiar un malware sin ejecutarlo, esto se debe analizar mediante herramientas como OllyDbg.

El análisis dinámico es más sencillo pues se basa en analizar el software mientras se está ejecutando, esto en una máquina virtual para no dañar nuestro propio dispositivo.

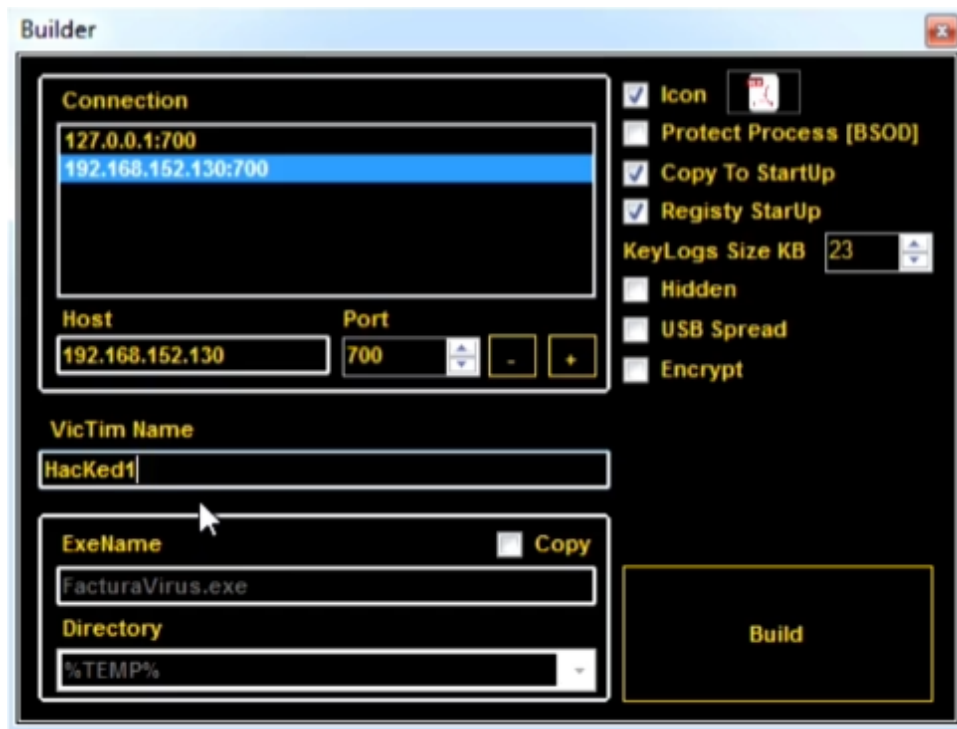
Tras analizar un ejecutable si detectamos actividad sospechosa debemos subirlo a plataformas como kaspersky o virus total para obtener más información



| DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY |
|-------------------|------------------------------------|-----------|------------------|---|
| Ad-Aware | ① Application.Agent.IAQ | | Avira (no cloud) | ① PUA/AD.InstallCore.gfiq |
| BitDefender | ① Application.Agent.IAQ | | Cylance | ① Unsafe |
| Cyren | ① W32/Application.KZDC-7426 | | DrWeb | ① Trojan.InstallCore.3612 |
| Emsisoft | ① Application.InstallCore (A) | | Endgame | ① Malicious (moderate Confidence) |
| eScan | ① Application.Agent.IAQ | | ESET-NOD32 | ① Win32/InstallCore.AYH Potentially Unwa... |
| F-Secure | ① PotentialRisk.PUA/AD.InstallCore | | Fortinet | ① Riskware/PUP.Installer |
| GData | ① Application.Agent.IAQ | | K7AntiVirus | ① Adware (005519851) |
| K7GW | ① Adware (005519851) | | Malwarebytes | ① PUP.Optional.InstallCore.Generic |
| MAX | ① Malware (ai Score=77) | | McAfee | ① PUP.Installer |
| McAfee-GW-Edition | ① PUP.Installer | | Microsoft | ① PUA.Win32/InstallCore |

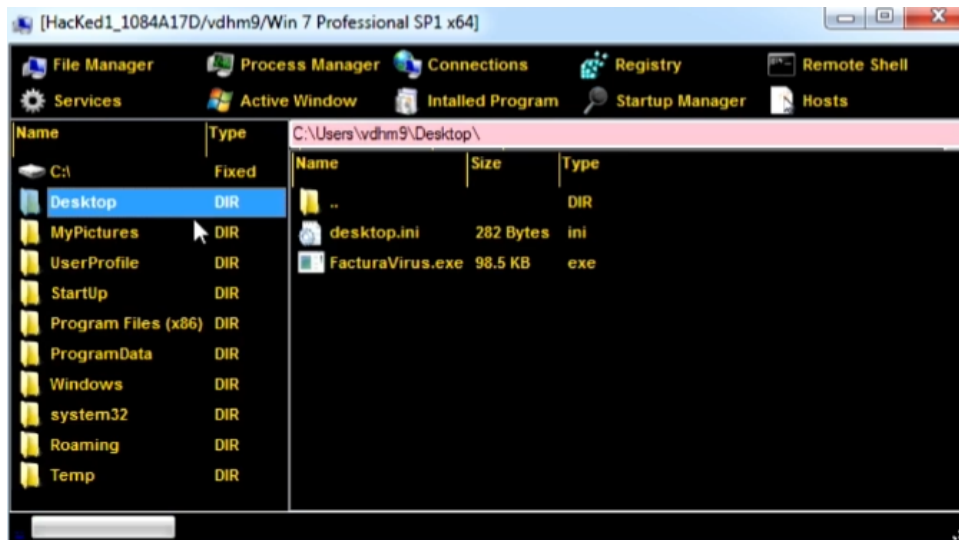
En esta imagen podemos ver como el ejecutable en cuestión es detectado por distintos antivirus y si nos fijamos más podremos ver que se trata de un troyano.

También se nos muestra la facilidad de crear software malicioso mediante la ayuda de aplicaciones como njRat



Aquí un ejemplo de cómo se crea un virus

Con este virus una vez la víctima lo ejecuta podremos ver todo lo que tiene en su ordenador así como tomar el control de la misma.



Aquí un ejemplo de ello