



Sandcastle: Analysis Summary



Sample Name: MegaVirus.exe

SHA-256: 45cbc47e3d510ad8716974629391b94e232b0816dcaf1d5ba44b580a99617b43

>> Analysis Results:

Designation: **MALWARE**

Analysed 30th Nov, 2021, 15:29:23

Threat level: 4/5

Sandbox OS: Windows-7-6.1.7601-SP1

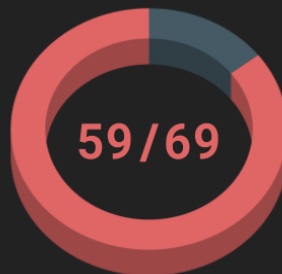
>> In Summary:

Overall, the sample
was found to be:



MALICIOUS

VirusTotal: Flagged
as **malicious** by:



Security Vendors

Something Something
online analysis



corruption



Insights //>>

- **MegaVirus.exe** is likely a Trojan Horse & Downloader.
- **Stealth Technique:** **MegaVirus.exe** disguises itself as a Chrome Addon.
- **Behaviour:** **MegaVirus.exe** likely makes outbound network connections.
- **Stealth Technique:** **MegaVirus.exe** is packed using UPX.
- **Some Other Insight:** Idk what to put here lol



Report Contents //>>

-\\ Clickable Chapter	Pg.
I. Sample Details	4
II. Imports	5
III. Strings	6
IV. VirusTotal Report	7
V. Online Sandbox Analysis	8



Sample Details //>>

Sample Name: MegaVirus.exe

MD5: b89670b6816d24c012bf4944e10764ff

SHA-1: 2c0009b6925b037e661fe50070a2abcdd076dee4

SHA-256: 45cbc47e3d510ad8716974629391b94e232b0816dcaf1d5ba44b580a99617b43

SS-DEEP: 768:vGBQHW7nVIWlaI8Bs43MHPQyaONTvY5Tqpy:rIWIWlQsgOe5T
