Based on the ARCHITECTURE of the binary, is malbuster_1 a 32-bit or a 64-bit application? (32-bit/64-bit)

32-bit ✓ Correct Answer

What is the MD5 hash of malbuster_1?

4348da65e4aeae6472c7f97d6dd8ad8f ✓ Correct Answer

Using the hash, what is the number of detections of malbuster_1 in VirusTotal?

62 ✓ Correct Answer

Based on VirusTotal detection, what is the malware signature of malbuster_2 according to Avira?

HEUR/AGEN.1306860 ✓ Correct Answer

malbuster_2 imports the function **_CorExeMain**. From which DLL file does it import this function?

mscoree.dll ✓ Correct Answer

Based on the VS_VERSION_INFO header, what is the original name of malbuster_2?

7JYpE.exe ✓ Correct Answer

Using the hash of malbuster_3, what is its malware signature based on abuse.ch?

TrickBot ✓ Correct Answer

Zloader ✓ Correct Answer

What is the message found in the DOS_STUB of malbuster_4?

!This Salfram cannot be run in DOS mode. ✓ Correct Answer

malbuster_4 imports the function **ShellExecuteA**. From which DLL file does it import this function?

shell32.dll ✓ Correct Answer

Using capa, how many anti-VM instructions were identified in malbuster_1?

3 ✓ Correct Answer

Using capa, which binary can log keystrokes?

malbuster_3 ✓ Correct Answer Hint

Using capa, what is the MITRE ID of the DISCOVERY technique used by malbuster_4?

T1083 ✓ Correct Answer

Which binary contains the string GodMode?

malbuster_2 ✓ Correct Answer

Which binary contains the string **Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)**?

malbuster_1 ✓ Correct Answer

3 ✓ Correct Answer

Using capa, which binary can log keystrokes?

malbuster_3 ✓ Correct Answer Hint

Using capa, what is the MITRE ID of the DISCOVERY technique used by malbuster_4?

T1083 ✓ Correct Answer

Which binary contains the string GodMode?

malbuster_2 ✓ Correct Answer

Which binary contains the string **Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)**?

malbuster_1 ✓ Correct Answer