Search for windows process filenames or hashes **Search**

msbuild.exe Source: Wild

Summary

MSBuild.exe is Microsoft's Build Engine. It is a platform used to build applications and is part of Microsoft Visual Studio. Visual Studio depends on MSBuild, but MSBuild can also be used independently.

EchoTrail Prevalence Score (EPS)

30.48

Rank Analysis

Host Prevalence

2.1%

Execution Rank

1,523rd

Behavioral Analysis

Top Hashes

e92325c4ae73cefeb2ec0c238bfc78´	38.06 %

More features and access with an account

Top Paths

C:\Program Files (x86)\Microsoft Visu:	37.88 %

More features and access with an account

Top Network Ports

8000	100.00 %

More features and access with an account

Ancestry Analysis

Top GrandParents

explorer.exe	32.79 %

More features and access with an account

Top Parents

devenv.exe	85.07 %

More features and access with an account

Top Children

VBCSCompiler.exe	39.37 %

More features and access with an account

Security Analysis

Intel

Given MSBuild's ability to process higher level code (e.g. C++ and .NET) on the fly, it has become a popular native Windows tool being leveraged during advanced attacks and pentests. It is sometimes found in malicious activity involving the compiling or running of malware. One common method of compiling and running malicious code using MSBuild is to provide it with a malicious .csproj file, which can be seen in the abused MSBuild's command line. Examining what processes are launched by a suspicious MSBuild process can help one infer what the suspicious code is doing.