DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

RAPORT
21.03.2022
UNCLASSIFIED / NECLASIFICAT

Situație site-uri cu activitate în contextul crizei Ucraina - Rusia, plus adrese IP specifice utilizate în atacuri malware

A. Lista site-uri fake news, fraude și / sau atacuri în contextul crizei Ucraina - Rusia

	URL / site	Tip / IP / Type	Status
1.	https://bitinitiators.com/blog.html	Frauda & Fake News - 23.111.123.188 - Rusia	Indisponibil la acest moment
2.	https://yourincome.site/LP/lp_RO_RO_connera_XfZdkl_Av0VP/?domain=newsmoney.work&uclick=q5fnx99z&uclickhash=q5fnx99z-q5fnx99z-qn-0-ydi4-cig5-usx90-f5491e	Frauda & Fake News - (fake HotNews) 188.166.109.10 - Olanda	Indisponibil la acest moment
3.	https://profitsmall.com/?domain=https://bitinitiators.com/blog	Frauda & Fake News - 23.111.123.188 - Rusia	Indisponibil la acest moment
4.	https://ru.md.sputniknews.com/	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - 178.248.234.83 - Rusia	Indisponibil la acest moment
5.	https://md.sputniknews.com/	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - 178.248.234.83 - Rusia	Indisponibil la acest moment
6.	https://ro.md.sputniknews.com/	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - 178.248.234.83 - Rusia	Indisponibil la acest moment
7.	https://citestesitu.com	Fake News - 207.180.255.212 - Germania	Indisponibil la acest moment
8.	https://rtnews.ro	Fake News - 161.97.93.67 - Germania	Indisponibil la acest moment
9.	https://cloudx.ro	Fake News - 164.68.101.156 - Germania	Indisponibil la acest moment
10.	https://russian.rt.com/	Fake News - 185.178.208.120 - Rusia	ACTIV
11.	https://www.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022: RT - Russia Today în engleză, RT - Russia Today Regatul Unit, RT - Russia Today Germania, RT - Russia Today Franța, RT - Russia Today în spaniolă	ACTIV
12.	RT - Russia Today Android	Idem - aplicație pe Google Play	Indisponibil la acest moment
13.	RT - Russia Today iOS	Idem	Indisponibil la acest moment
14.	RT - Russia Today HarmonyOS	Idem	Indisponibil la acest moment
15.	Sputnik Android	Idem - aplicație pe Google Play	Indisponibil la acest moment
16.	Sputnik iOS	Idem	Indisponibil la acest moment
17.	Sputnik HarmonyOS	Idem	Indisponibil la acest moment
18.	www.doilupi.ro	Idem - 77.81.2.84 - România, Maramureș	Indisponibil la acest moment
19.	www.enterieur.ro	Idem - 89.39.246.12 - România, Sfântu-Gheorghe, Covasna	ACTIV
20.	francais.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - Russia Today în franceză 185.178.208.110 - Rusia	ACTIV
21.	popup.taboola.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - Russia Today pe Android 199.232.17.44 - Austria	ACTIV
22.	rt-news-gcm.firebaseio.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - Russia Today pe Android - United States (doar subdomeniul rt-news-gcm.firebaseio.com)	ACTIV
23.	rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - Russia Today în engleza 185.178.208.5 - Rusia	ACTIV
24.	push.dev.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - Russia Today pe Android 89.191.237.180 - Rusia	ACTIV
25.	radiort.rttv.ru	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 - Russia Today pe Android 109.73.15.235 - Rusia	ACTIV

	URL / site	Tip / IP / Type	Status
26.	de.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Russia Today in germană 185.178.208.109 - 185.79.236.190 - Rusia	ACTIV
27.	arabic.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Russia Today in arabă 185.79.236.173 - 185.178.208.111 - Rusia	ACTIV
28.	actualidad.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Russia Today în spaniolă 185.178.208.108 - Rusia	ACTIV
29.	doc.rt.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Russia Today pe Android 185.79.236.160 - Rusia	ACTIV
30.	sputnik-a5afd.firebaseio.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android - United States (doar subdomeniul sputnik-a5afd.firebaseio.com)	ACTIV
31.	a.sputniknews.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android 195.93.247.89, RU, Russian Federation	ACTIV
32.	rian.ru	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android 178.248.233.32, RU, Russian Federation	ACTIV
33.	mobileapi.sputniknews.com	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android 178.248.238.102, RU, Russian Federation	ACTIV
34.	mobilehit.ria.ru	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android 195.93.247.50, RU, Russian Federation	ACTIV
35.	mobileapi.ria.ru	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android 178.248.238.102, RU, Russian Federation	ACTIV
36.	mfd.rian.ru	Decizia (PESC) 2022/351 a Consiliului UE din 1 martie 2022 – Sputnik pe Android 178.248.233.32, RU, Russian Federation	ACTIV
37.	postal-romania.com	Phishing / impersonare domeniu Poșta Română 188.127.235.163 – Rusia - **hXXps://postal-romania.com/inregistr/bills/index2.php**	Indisponibil la acest moment

Legenda:

= raportate în zilele anterioare = raportări noi

NOTĂ: accesul utilizatorilor din România la domeniile și adresele de IP de mai sus poate fi oprit / restricționat utilizând resurse Internet din România, dar acestea pot fi încă accesate din afara țării utilizând servicii de tip VPN, TOR sau alte metode tehnice. Directoratul depune eforturi susținute pentru a asigura acuratețea datelor prezentate.

B. Lista de adrese IP de pe care sunt propagate atacuri cibernetice și malware ce pot impacta inclusiv România, în contextul crizei Ucraina – Rusia

	IP	Țara ISP ISP Country	Tip atac / incident Type of attack / incident	Observații / Observations
1.	100.43.220.234	USA / SUA	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
2.	105.159.248.137	Maroc	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
3.	109.192.30.125	Germania	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
4.	151.0.169.250	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
5.	185.82.169.99	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
6.	188.152.254.170	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
7.	2.230.110.137	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
8.	208.81.37.50	USA / SUA	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
9.	212.103.208.182	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
10.	212.202.147.10	Germania	Katana Botnet DDoS	ACTIV
11.	212.234.179.113	Franța	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
12.	217.57.80.18	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
13.	24.199.247.222	USA / SUA	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
14.	37.71.147.186	Franța	Katana Botnet DDoS	ACTIV
15.	37.99.163.162	Arabia Saudită	Katana Botnet DDoS	ACTIV
16.	5.182.211.5	Olanda	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
17.	50.255.126.65	USA / SUA	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
18.	70.62.153.174	USA / SUA	Katana Botnet DDoS	ACTIV
19.	78.134.89.167	Italia	Katana Botnet DDoS	ACTIV
20.	80.15.113.188	Franța	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
21.	80.153.75.103	Germania	Katana Botnet DDoS	ACTIV
22.	80.155.38.210	Germania	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
23.	81.4.177.118	Cipru	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
24.	90.63.245.175	Franța	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
25.	93.51.177.66	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
26.	96.80.68.193	USA / SUA	Katana Botnet DDoS	ACTIV
27.	91.240.118.117	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
28.	91.240.118.119	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
29.	91.240.118.121	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
30.	91.240.118.123	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
31.	95.167.212.219	Rusia	Port Scanning	ACTIV
32.	95.163.255.59	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
33.	95.163.255.57	Rusia	Vulnerability scan	ACTIV
34.	95.163.255.55	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
35.	95.163.255.18	Rusia	Brute Force	Indisponibil din RO la momentul raportării
36.	95.163.255.13	Rusia	Brute Force	Indisponibil din RO la momentul raportării
37.	95.163.255.12	Rusia	Brute Force	Indisponibil din RO la momentul raportării
38.	95.163.12.113	Rusia	Port Scanning	ACTIV
39.	93.158.228.230	Rusia	Port Scanning	ACTIV
40.	92.63.196.61	Rusia	Vulnerability scan	ACTIV
41.	89.188.166.225	Rusia	Port scan/probing	ACTIV
42.	88.147.189.62	Rusia	Unauthorized acces	Indisponibil din RO la momentul raportării
43.	5.8.10.202	Rusia	Mailserver/account/attacks	ACTIV
44.	5.188.88.178	Rusia	Port Scanning	Indisponibil din RO la momentul raportării
45.	5.188.210.227	Rusia	Brute Force	ACTIV
46.	5.188.210.158	Rusia	Port Scanning	ACTIV
47.	45.146.165.37	Rusia	Brute Force	ACTIV
48.	37.9.45.49	Rusia	Port Scanning	Indisponibil din RO la momentul raportării
49.	217.107.219.12	Rusia	Port Scanning	ACTIV
50.	213.171.58.162	Rusia	Port Scanning	ACTIV
51.	213.141.153.218	Rusia	Port Scanning	ACTIV
52.	194.26.29.120	Rusia	Port Scanning	ACTIV
53.	188.16.148.85	Rusia	Port Scanning	ACTIV
54.	185.94.111.1	Rusia	Port Scanning	ACTIV
55.	185.20.226.243	Rusia	Port Scanning	ACTIV
56.	178.46.213.113	Rusia	Port Scanning	Indisponibil din RO la momentul raportării
57.	178.176.194.62	Rusia	Port Scanning	ACTIV
58.	176.124.192.4	Rusia	Port Scanning	ACTIV
59.	109.95.198.12	Rusia	Port Scanning	ACTIV
60.	109.226.220.205	Rusia	Port Scanning	ACTIV
61.	185.154.53.46	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării

	IP	Țara ISP ISP Country	Tip atac / incident Type of attack / incident	Observații / Observations
62.	109.237.96.124	Rusia	Vulnerability scan	ACTIV
63.	84.201.241.141	Rusia	Botnet	Indisponibil din RO la momentul raportării
64.	109.237.103.9	Rusia	WebApp Scanning	ACTIV
65.	185.153.196.97	Rusia	Trojan backdoor	Indisponibil din RO la momentul raportării
66.	5.188.211.15	Rusia	VEX Webshell	ACTIV
67.	5.188.211.35	Rusia	VEX Webshell	ACTIV
68.	5.188.211.22	Rusia	Vulnerability scan	ACTIV
69.	46.161.11.4	Rusia	Web App Attack	ACTIV
70.	81.177.139.223	Rusia	Troian Gen:Variant.Kazy	ACTIV
71.	92.53.116.200	Rusia	Virus W32 Virut	ACTIV
72.	95.143.178.136	Rusia	Web App Attack / Brute-Force	ACTIV
73.	185.193.127.179	Finlanda	Web App Attack / Brute-Force	Indisponibil din RO la momentul raportării
74.	159.223.64.156	Singapore	Web App Attack / Brute-Force	ACTIV
75.	217.77.209.242	Ucraina	Vulnerability scan	ACTIV
76.	89.189.128.224	Rusia	Brute-Force	ACTIV
77.	109.188.93.139	Rusia	Brute-Force	ACTIV
78.	5.252.119.68	Rusia	Brute-Force	Indisponibil din RO la momentul raportării
79.	85.249.53.189	Rusia	Brute-Force	Indisponibil din RO la momentul raportării
80.	89.113.143.62	Rusia	Brute-Force	Indisponibil din RO la momentul raportării
81.	89.109.45.170	Rusia	Brute-Force	Indisponibil din RO la momentul raportării
82.	85.143.223.167	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
83.	87.246.7.246	Bulgaria	Brute-Force	ACTIV
84.	87.246.7.229	Bulgaria	Brute-Force	ACTIV
85.	79.124.62.82	Bulgaria	Vulnerability scan	ACTIV
86.	79.124.62.78	Bulgaria	Vulnerability scan	ACTIV
87.	79.124.62.130	Bulgaria	Vulnerability scan	ACTIV
88.	79.124.62.110	Bulgaria	Vulnerability scan	ACTIV
89.	79.124.62.86	Bulgaria	Vulnerability scan	ACTIV
90.	79.124.62.34	Bulgaria	Vulnerability scan	ACTIV
91.	122.96.25.198	China	Web App Attack	Indisponibil din RO la momentul raportării
92.	120.85.119.58	China	Web App Attack	Indisponibil din RO la momentul raportării
93.	79.131.184.190	Grecia	Web App Attack	Indisponibil din RO la momentul raportării
94.	64.6.64.6	USA / SUA	Vulnerability scan	ACTIV
95.	46.17.102.83	Olanda	Vulnerability scan	Indisponibil din RO la momentul raportării
96.	81.177.143.31	Rusia	Vulnerability scan	ACTIV
97.	194.26.29.195	Rusia	Vulnerability scan	ACTIV
98.	91.240.118.73	Rusia	Vulnerability scan	ACTIV
99.	91.240.118.75	Rusia	Vulnerability scan	ACTIV
100.	91.240.118.71	Rusia	Vulnerability scan	ACTIV
101.	194.26.29.169	Rusia	Vulnerability scan	ACTIV
102.	45.143.200.50	Rusia	Vulnerability scan	ACTIV
103.	91.240.118.77	Rusia	Vulnerability scan	ACTIV
104.	92.63.196.25	Rusia	Vulnerability scan	ACTIV
105.	45.143.203.3	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
106.	193.201.9.161	Rusia	Vulnerability scan	ACTIV
107.	45.146.165.165	Rusia	Vulnerability scan	ACTIV
108.	193.3.19.119	Rusia	Vulnerability scan	ACTIV
109.	193.3.19.156	Rusia	Vulnerability scan	ACTIV
110.	185.191.34.144	Rusia	Vulnerability scan	ACTIV
111.	193.3.19.33	Rusia	Vulnerability scan	ACTIV
112.	185.151.147.249	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
113.	185.151.147.248	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
114.	62.233.50.55	Rusia	Vulnerability scan	ACTIV
115.	31.44.185.237	Rusia	Vulnerability scan	ACTIV
116.	185.248.101.71	Rusia	Vulnerability scan	ACTIV
117.	45.143.200.114	Bulgaria	Port Scanning / Brute-Force	ACTIV
118.	188.127.235.163	USA / SUA	Phishing	ACTIV
119.	103.107.104.19	Hong Kong	Phishing	ACTIV
120.	45.154.14.235	Coreea de Sud	Phishing	Indisponibil din RO la momentul raportării
121.	69.90.184.125	USA / SUA	Phishing	Indisponibil din RO la momentul raportării
122.	92.118.188.78	USA / SUA	Phishing	ACTIV
123.	176.118.165.121	Rusia	Vulnerability scan	Indisponibil din RO la momentul raportării
124.	185.156.73.91	Rusia	Vulnerability scan	ACTIV
125.	94.232.45.43	Rusia	Vulnerability scan	ACTIV
126.	162.62.191.220	Rusia	Vulnerability scan	ACTIV
127.	43.131.68.225	Rusia	Vulnerability scan	ACTIV
128.	43.131.94.145	Rusia	Vulnerability scan	ACTIV

	IP	Țara ISP ISP Country	Tip atac / incident Type of attack / incident	Observații / Observations
129.	162.62.33.200	Rusia	Vulnerability scan	ACTIV
130.	162.62.191.231	Rusia	Vulnerability scan	ACTIV
131.	43.131.66.209	Rusia	Vulnerability scan	ACTIV
132.	45.146.164.88	Rusia	Vulnerability scan	ACTIV
133.	43.131.91.178	Rusia	Vulnerability scan	ACTIV
134.	45.143.200.114	Rusia	Vulnerability scan	ACTIV
135.	78.128.113.46	Bulgaria	Vulnerability scan	ACTIV
136.	46.148.20.13	Ucraina	Vulnerability scan	ACTIV
137.	77.120.110.150	Ucraina	Vulnerability scan	Indisponibil din RO la momentul raportării
138.	183.17.63.170	China	Vulnerability scan	Indisponibil din RO la momentul raportării
139.	117.50.179.151	China	Brute-Force	ACTIV
140.	117.50.178.176	China	Brute-Force	Indisponibil din RO la momentul raportării
141.	183.17.56.55	China	Brute-Force	ACTIV
142.	159.75.134.236	China	Brute-Force	ACTIV
143.	139.224.75.74	China	Brute-Force	ACTIV
144.	124.65.132.134	China	Web App Attack	ACTIV
145.	120.229.2.65	China	Web App Attack	ACTIV
146.	115.28.139.184	China	Web App Attack	ACTIV
147.	78.128.113.34	Bulgaria	Vulnerability scan	ACTIV
148.	85.202.169.181	Olanda	Brute-Force	ACTIV
149.	27.194.236.44	China	Mirai Scan si Web App Attack	ACTIV
150.	176.119.2.212	Ucraina	Malware SPECTR	Indisponibil din RO la momentul raportării
151.	176.119.2.214	Ucraina	Malware SPECTR	Indisponibil din RO la momentul raportării
152.	176.119.5.194	Ucraina	Malware SPECTR	Indisponibil din RO la momentul raportării
153.	176.119.5.195	Ucraina	Malware SPECTR	Indisponibil din RO la momentul raportării
154.	45.95.11.34	Slovacia	Phishing	Indisponibil din RO la momentul raportării

Legenda:

= raportate în zilele anterioare = raportări noi

NOTĂ: accesul utilizatorilor din România la domeniile și adresele de IP de mai sus poate fi oprit / restricționat utilizând resurse Internet din România, dar acestea pot fi încă accesate din afara țării utilizând servicii de tip VPN, TOR sau alte metode tehnice. Directoratul depune eforturi susținute pentru a asigura acuratețea datelor prezentate.

C. Lista de domenii, site-uri web și / sau adrese IP pentru care s-au implementat măsuri de remediere și verificare ce permit ridicarea limitărilor și restricțiilor

Pentru următorul domeniu și adresă IP, Directoratul confirmă implementarea măsurilor de remediere și verificare ce permit anularea limitărilor sau restricțiilor:

bookblog.ro și **IP 128.140.228.210**

Directoratul și reprezentanții domeniului **bookblog.ro** s-au coordonat pentru a analiza toate aspectele relevante cu privire la plasarea domeniului menționat pe lista resurselor implicate în atacuri cibernetice tip DDoS asupra unor instituții guvernamentale din UE desfășurate în contextul crizei Ucraina – Rusia. Printre măsurile de remediere și verificare discutate și efectuate:

- Schimbarea serviciului de hosting utilizat pentru **bookblog.ro** – un nou serviciu de la un nou furnizor
- Schimbarea serviciului DNS – a fost schimbat furnizorul de servicii DNS
- Instalarea unei noi versiuni a platformei Wordpress folosită de **bookblog.ro**
- Instalarea unor versiuni noi și actualizate ale tuturor plug-in-urilor folosite
- Schimbarea tuturor parolelor pentru toate conturile de Administrator/Editor folosite
- Verificarea conținutului de fișiere al site-ului vechi pentru a detecta fișierele modificate
- Efectuarea unei analize a vulnerabilităților de securitate cibernetică ale platformei
- Informarea de către Directorat a partenerilor internaționali din CSIRT Network cu privire la implementarea măsurilor de remediere și verificare pentru **bookblog.ro** și **IP-ul 128.140.228.210**

DISCLAIMER

Listele de mai sus au fost pregătite pe baza informației colectate din surse tehnice si non-tehnice aflate la dispoziția Directoratului, la momentul publicării. Listele sunt dinamice și pot suferi modificări rapide, în funcție de acțiunile și deciziile specifice derulate în spațiul cibernetic sau luate de către autoritățile competente.

The above lists have been prepared on the basis of information collected from technical and non-technical sources available to the Directorate at the time of publication. The lists are dynamic and may rapidly change, depending on the specific actions and decisions taken in cyberspace or those taken by the competent authorities.

Наведені вище списки підготовлені на основі інформації, зібраної з технічних та нетехнічних джерел, доступних Директорату на момент публікації. Списки є динамічними і можуть швидко змінюватися залежно від конкретних дій і рішень, прийнятих у кіберпросторі або компетентними органами.

Вышеприведенные списки были подготовлены на основе информации собранной из технических и нетехнических источников, доступные Руководсту на момент публикации. Списки являются динамическими и могут быстро меняться в зависимости от конкретных действий и решений, предпринятых в киберпространстве или принятых компетентными органами.
