DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

RAPORT
03.03.2022
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 și fraude cu activitate 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 - Netherlands	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/	Fake News 178.248.234.83 - Rusia	Indisponibil la acest moment site găzduit în Rusia
5.	https://md.sputniknews.com/	Fake News 178.248.234.83 - Rusia	Indisponibil la acest moment site găzduit în Rusia
6.	https://ro.md.sputniknews.com/	Fake News 178.248.234.83 - Rusia	Indisponibil la acest moment site găzduit în Rusia
7.	https://citestesitu.com	Fake News 207.180.255.212 - Germania	Indisponibil la acest moment site găzduit în Germania
8.	https://rtnews.ro	Fake News 161.97.93.67 - Germania	Indisponibil la acest moment site găzduit în Germania
9.	https://cloudx.ro	Fake News	Indisponibil la acest moment
10.	https://www.aktual24.ro	Fake News IP 148.251.128.74 - Germania IP 148.251.128.158 - Germania	ACTIV
11.	https://russian.rt.com/	Fake News 185.178.208.120 - Rusia	ACTIV

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.

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	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	ACTIV
6.	188.152.254.170	Italia	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
7.	2.230.110.137	Italia	Katana Botnet DDoS	ACTIV
8.	208.81.37.50	USA	Katana Botnet DDoS	ACTIV
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	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	Katana Botnet DDoS	Indisponibil din RO la momentul raportării
18.	70.62.153.174	USA	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	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	ACTIV
33.	95.163.255.57	Rusia	Vulnerability scan	ACTIV
34.	95.163.255.55	Rusia	Vulnerability scan	ACTIV
35.	95.163.255.18	Rusia	Brute Force	ACTIV
36.	95.163.255.13	Rusia	Brute Force	ACTIV
37.	95.163.255.12	Rusia	Brute Force	ACTIV
38.	95.163.12.113	Rusia	Port Scanning	ACTIV
39.	93.158.228.230	Rusia	Port Scanning	Indisponibil din RO la momentul raportări
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	ACTIV
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	Indisponibil din RO la momentul raportării
54.	185.94.111.1	Rusia	Port Scanning	Indisponibil din RO la momentul raportării
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	Indisponibil din RO la momentul raportării
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	ACTIV
62.	109.237.96.124	Rusia	Vulnerability scan	ACTIV
63.	84.201.241.141	Rusia	Botnet	ACTIV

	IP	Țara ISP ISP Country	Tip atac / incident Type of attack / incident	Observații / Observations
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

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.

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.
