

Перечень индикаторов компрометации

Сетевые индикаторы компрометации	
thisbusylife[.]com	
yiars[.]com	
energosale34[.]download	
pdfbypari[.]com	
abxweb[.]com	
80[.]66[.]76[.]115	
80[.]78[.]24[.]5	
94[.]232[.]43[.]219	
23[.]254[.]243[.]67	
80[.]78[.]27[.]201	
hxxps[:]//thisbusylife[.]com/line/call[.]php	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/Povestka_34	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/catchange_banner_tg[.]jpeg	
hxxps[:]//energosale34[.]download/Downloads/Anketa_energосale[.]docx[.]lnk	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/povestka_378478112[.]pdf	
hxxps[:]//thisbusylife[.]com/updtr[.]php	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/Anketa_energосale[.]docx	
hxxp[:]//80[.]78[.]27[.]201/Downloads/povestka_378478112[.]pdf[.]lnk	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/tz_ads[.]pdf	
hxxps[:]//thisbusylife[.]com/abpf/	
hxxps[:]//yiars[.]com/stap/checkin[.]php	
hxxps[:]//yiars[.]com/gzz/gz_all[.]zip	
hxxps[:]//yiars[.]com/update[.]php	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/T3_CatChange[.]txt	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/Anketa1	
hxxp[:]//80[.]78[.]24[.]5/Downloads/Anketa_energосale[.]docx[.]lnk	
hxxp[:]//80[.]66[.]76[.]115/fakeurl[.]htm	
hxxp[:]//94[.]232[.]43[.]219/fakeurl[.]htm	
hxxps[:]//github[.]com/NonaDoc/Nonadoc/releases/download/defi_privе/Anketa_energосale	
hxxps[:]//thisbusylife[.]com/abpz/abp_all[.]zip	Министерство цифрового развития и связи Свердловской области 11.12.2024 Вх.№ 16530

Файловые индикаторы компрометации (sha256)

8762d87be2998ca50229e9b51a2a7700bbb1fd75b99864d05b4d630a5e091014
 26be491b59e98932bf12985cd6a24d5a0be33ee92767b19b41fe2917deb96f79
 0bac7153fa7a9a5e72d7df918c467c329fd7a78dcfdb67797592ad6c71cffa4b
 df9c9778ebb2b7b59dce74c1c10eeb81dad29075a486ab11f782126715f4c965
 68d0373fc7fcd74d7379f8175a894194ac285f98810359a7f48978ef15f5283e
 b0d738f7003d5bb5d7c5d0dc9441e45367fad635cbf505f129df48f8155e38a2
 1b57ab2cfd892f0eda60dddcbbfc0bc0214dd556a7030f4cd77f9141920b1f72d
 6c5f008cb1a9c8bf26720c76622d95ff82cd1e6cb682755df17e7131ea493eea
 96bd372f8a4e39e0e6e629994a2b284432c9e5a0a48e1f46100a0a6b0ce349bd
 b1e16f4b12abfffc6eaa6abc6861108c255158fb0baa4d50fb7de799d463c340
 0af90212ce3cdb4d7e9fb18c0da57a33533481fab4d9f0ca5beebd1991ba75cf
 25d923a04b40403fdf337be6a6fe6dbd6f84bf4e1897ba09573661f73827a800
 40f34fc1f8768e0c2e665a1bf589c4f4a650d642fe93f8e01334e80a3085e271
 fde8b56d6d84dd0d361f011ad37426b166ab4cbe910388eb011a6590ec39c897
 b856e4c802e07686fccd564cfe47e705421c4e5605bce540299f16e338f9c556
 176f7e61d26c33df91425f063c6494d6cd63f4de2654de3d72158a272bb03ae5
 90301696accc600a3fc2a1419d0c73566a19f42424d2da6e6f215a83ba3895e6
 86e187b90179bd9edc49a37cb53e3444a589ef8fa1eb00544cc9fa31f7313ce3
 5ca68818d816869b96aef284efc2429e61d11ce2332a2de8bc4cc3bef64fd834
 9d405c3a3bd95031175b1f36b485a5210fd499155fa0db0403a81f3af928a271
 885dfbeecbc41e2e5ecb6f1148d0f1c01e1b7d862ed3e9698669dce652339515