Fm: Cyber Warfare Center Pacific (CYWAR-CENPAC)
Annex: Liberty Station USNTC Point Loma PACCOM
UPDATE: Russian Unified Energy System
Release: General/Sensitive/NOFORN
By: Brig. M. Lindsey, Chief U2 Force HQ
Dated: 09/13/2024 03:33 Zulu

The following content was collected and assessed pursuant to a good faith effort for a legitimate purpose using an identifiable interface, activity that is fully documented and performed without financial compensation or personal gain, as per US DOJ guidelines.

Russia has a centralized system for coordinating its national electrical grid. The Unified Energy System (UES) of Russia manages the majority of the country's electricity generation, transmission, and distribution. The UES is operated by System Operator of the Unified Energy System (SO UES), a state-owned company responsible for the centralized dispatching of electricity across the national grid. This organization ensures the stability, security, and coordination of the grid across Russia's vast territory.

The SO UES oversees 69 regional dispatch centers and coordinates with generating plants, transmission companies, and distribution networks to manage the real-time balance of electricity supply and demand. It plays a critical role in monitoring the grid's reliability, especially during times of high demand or emergency situations, and has been instrumental in maintaining grid stability across different regions of Russia.

Additionally, the grid's operations are influenced by Russia’s Federal Grid Company (FGC), which owns and operates the high-voltage transmission lines across the country.

This centralized coordination is vital given the geographic expanse and varying energy demands across Russia's regions.

The System Operator of the Unified Energy System (SO UES), which manages the Russian national grid, is headquartered in Moscow, Russia. The company is responsible for the centralized dispatch control of electricity production and transmission throughout the country.

Their headquarters coordinates the operation of numerous regional dispatch centers to maintain a stable and secure electrical supply across Russia. The Moscow location enables it to act as the core point for managing the national energy grid, given the city's infrastructure and governmental proximity.

Its headquarters at the following address in Moscow:

5 Akademika Chelomeya Street, Moscow, Russia, 117630.

This is where the main dispatching center is located, which manages and monitors the real-time operations of the grid across Russia. The facility plays a critical role in ensuring the grid's stability and efficiency.

https://tadviser.com/index.php/Company:SO_UES_-_System_Operator_of_the_Unified_Energy_System

The System Operator of the Unified Energy System (SO UES) of Russia is responsible for managing a wide range of critical infrastructure related to the national electrical grid.

1. Power Generation Coordination: SO UES coordinates the dispatch of electricity from various power plants across Russia. This includes:

- Thermal power plants (coal, gas, oil)
- Nuclear power plants

Hydroelectric power stations
Renewable energy sources (wind, solar, etc.)

2. Transmission Lines: The organization oversees the operation of high-voltage transmission lines that transport electricity across vast distances. Russia’s grid includes ultra-high voltage lines (up to 1,150 kV) that ensure stable power delivery from remote generating stations to population centers. These lines are part of Russia's Federal Grid, maintained by the Federal Grid Company.

3. Regional Dispatch Centers: In addition to the central dispatch office in Moscow, SO UES manages 69 regional dispatch centers across Russia. These centers oversee localized grid operations and respond to specific energy demands, ensuring that power is distributed efficiently within different regions.

4. Substations and Transformers: SO UES is responsible for managing substations and transformers, which are crucial for stepping up or stepping down voltage as electricity moves from power plants to end users. These facilities ensure that electricity is safely transmitted over long distances and then distributed locally.

5. Grid Monitoring and Control Systems: SO UES operates advanced real-time monitoring and control systems that oversee the status of the grid, forecast energy demands, and prevent outages or overloads. These systems are critical for maintaining the balance between electricity supply and demand, particularly in extreme weather or emergency situations.

6. Interconnection with Neighboring Grids: Russia’s electrical grid is connected to neighboring countries’ grids, including those of Belarus, Kazakhstan, and Finland. SO UES helps manage these international interconnections, ensuring the seamless exchange of power across borders when necessary.

This vast and complex infrastructure allows SO UES to maintain grid stability, meet the country's energy demands, and manage emergency responses to ensure continuous power supply.

SO UES is PJSC FGC UES whose network is AS59846 and the SO UES branch network is AS39073/branch route 195.66.72.0/24 Trunk Power Grid Northwest Moscow. AS59846 is the autonomous network hub for 655 power grid infrastructure and power generation facilities in the Russian Federation that all are peered through PJSC Vimpelcom AS3216 using DNS:

195.66.72.15	owa.ural.fsk-ees.ru	

195.66.72.19	ur-hq-dns-02.ural.fsk-ees.ru	
195.66.72.20	ur-hq-dns-01.ural.fsk-ees.ru	
195.66.72.26	ur-hq-mr-02.ural.fsk-ees.ru	
195.66.72.27	ur-hq-mr-01.ural.fsk-ees.ru	

The main domain is fsk-ees.ru (195.66.72.4) AS39073 in Yekaterinburg, Russia. The individual real-time feeds as follows:

net	IP	Peer		Origin
rrc00.ripe.net	80.77.16.114	34549	x	39073
rrc00.ripe.net	45.14.68.69	206499	x	39073
rrc00.ripe.net	198.58.198.252	1403	x	39073
rrc00.ripe.net	161.129.152.2	13830	x	39073
rrc00.ripe.net	49.12.70.222	44393	x	39073
rrc00.ripe.net	194.50.19.4	202365	x	39073
rrc00.ripe.net	64.246.96.5	20205	x	39073
rrc00.ripe.net	2a09:4c0:100:5eb1::7afb	58057	x	39073
rrc00.ripe.net	45.134.89.1	34927	x	39073
rrc00.ripe.net	193.160.39.1	57821	x	39073
rrc00.ripe.net	208.51.134.248	3549	x	39073
rrc00.ripe.net	185.102.84.232	61218	x	39073
rrc00.ripe.net	45.116.179.212	55720	x	39073
rrc00.ripe.net	203.119.104.1	4608	x	39073
rrc00.ripe.net	193.163.86.231	34800	x	39073
rrc00.ripe.net	5.255.90.109	202365	x	39073
rrc00.ripe.net	94.177.122.251	58057	x	39073
rrc00.ripe.net	178.208.11.4	50628	x	39073
rrc00.ripe.net	208.80.153.193	14907	x	39073

rrc00.ripe.net	12.0.1.63	7018	x	39073
rrc00.ripe.net	165.254.255.2	15562	x	39073
rrc00.ripe.net	185.193.84.191	29504	x	39073
rrc00.ripe.net	45.61.0.85	22652	x	39073
rrc00.ripe.net	89.234.186.6	204092	x	39073
rrc00.ripe.net	194.28.97.2	45049	x	39073
rrc00.ripe.net	194.50.92.251	58057	x	39073
rrc00.ripe.net	193.148.251.1	34927	x	39073
rrc00.ripe.net	31.169.49.228	50304	x	39073
rrc00.ripe.net	103.102.5.1	131477	x	39073
rrc00.ripe.net	217.151.205.144	20514	x	39073
rrc00.ripe.net	202.150.221.37	38001	x	39073
rrc00.ripe.net	2.56.11.1	34854	x	39073
rrc00.ripe.net	94.247.111.254	49673	x	39073
rrc00.ripe.net	91.212.242.251	49420	x	39073
rrc00.ripe.net	193.150.22.240	57381	x	39073
rrc00.ripe.net	176.12.110.8	50300	x	39073
rrc00.ripe.net	185.210.224.254	49432	x	39073
rrc00.ripe.net	5.178.95.254	59919	x	39073
rrc00.ripe.net	154.11.12.212	852	x	39073
rrc00.ripe.net	193.0.0.56	3333	x	39073
rrc00.ripe.net	202.69.160.152	17639	x	39073
rrc00.ripe.net	203.175.175.15	24482	x	39073
rrc03.ripe.net	80.249.210.78	59605	x	39073
rrc03.ripe.net	80.249.210.85	25160	x	39073
rrc03.ripe.net	80.249.210.134	34019	x	39073
rrc03.ripe.net	80.249.210.153	24482	x	39073
rrc03.ripe.net	80.249.209.53	8218	x	39073
rrc03.ripe.net	80.249.209.211	3320	x	39073
rrc03.ripe.net	80.249.211.237	19993	x	39073

		8		
rrc03.ripe.net	80.249.208.200	12859	x	39073
rrc03.ripe.net	80.249.208.208	12956	x	39073
rrc03.ripe.net	80.249.212.10	50629	x	39073
rrc03.ripe.net	80.249.210.150	199524	x	39073
rrc03.ripe.net	193.239.117.18	205206	x	39073
rrc03.ripe.net	193.239.116.60	399580	x	39073
rrc03.ripe.net	80.249.210.207	35598	x	39073
rrc03.ripe.net	80.249.208.34	1103	x	39073
rrc03.ripe.net	80.249.209.176	14907	x	39073
rrc03.ripe.net	193.239.116.202	212828	x	39073
rrc03.ripe.net	80.249.210.156	6233	x	39073
rrc03.ripe.net	80.249.211.161	8283	x	39073
rrc03.ripe.net	80.249.209.145	6908	x	39073
rrc03.ripe.net	80.249.210.163	51185	x	39073
rrc03.ripe.net	80.249.208.162	49544	x	39073
rrc03.ripe.net	80.249.208.209	51088	x	39073
rrc03.ripe.net	193.239.117.30	41047	x	39073
rrc03.ripe.net	80.249.208.106	6830	x	39073
rrc03.ripe.net	193.239.118.106	42541	x	39073
rrc03.ripe.net	80.249.211.217	8455	x	39073
rrc03.ripe.net	80.249.209.167	6453	x	39073
rrc03.ripe.net	80.249.208.122	6461	x	39073
rrc03.ripe.net	80.249.213.102	47147	x	39073
rrc03.ripe.net	80.249.208.149	15435	x	39073
rrc04.ripe.net	192.65.185.195	15547	x	39073
rrc04.ripe.net	192.65.185.244	25091	x	39073
rrc04.ripe.net	192.65.185.142	20932	x	39073
rrc04.ripe.net	192.65.185.157	12350	x	39073

rrc04.ripe.net	192.65.185.141	6730	x	39073
rrc04.ripe.net	192.65.185.140	29222	x	39073
rrc05.ripe.net	193.203.0.91	13237	x	39073
rrc05.ripe.net	193.203.0.63	6720	x	39073
rrc05.ripe.net	193.203.0.157	35369	x	39073
rrc05.ripe.net	193.203.0.182	48362	x	39073
rrc05.ripe.net	193.203.0.75	40994	x	39073
rrc05.ripe.net	193.203.0.213	51184	x	39073
rrc05.ripe.net	193.203.0.145	31510	x	39073
rrc05.ripe.net	193.203.0.45	8218	x	39073
rrc05.ripe.net	193.203.0.245	59890	x	39073
rrc05.ripe.net	193.203.0.192	47692	x	39073
rrc05.ripe.net	193.203.0.19	47147	x	39073
rrc06.ripe.net	202.249.2.185	25152	x	39073
rrc06.ripe.net	202.249.2.20	4777	x	39073
rrc06.ripe.net	202.249.2.83	2500	x	39073
rrc06.ripe.net	210.171.225.165	59105	x	39073
rrc06.ripe.net	202.249.2.169	2497	x	39073
rrc14.ripe.net	198.32.176.177	7575	x	39073
rrc14.ripe.net	198.32.176.24	2497	x	39073
rrc14.ripe.net	198.32.176.164	19151	x	39073
rrc14.ripe.net	198.32.176.3	1280	x	39073
rrc14.ripe.net	198.32.176.70	6762	x	39073
rrc14.ripe.net	198.32.176.226	199524	x	39073
rrc14.ripe.net	198.32.176.14	2914	x	39073
rrc15.ripe.net	187.16.216.209	28634	x	39073
rrc15.ripe.net	187.16.217.122	35280	x	39073
rrc15.ripe.net	187.16.220.216	52873	x	39073
rrc15.ripe.net	187.16.209.34	271253	x	39073
rrc15.ripe.net	187.16.217.17	22548	x	39073

rrc15.ripe.net	187.16.217.59	23106	x	39073
rrc15.ripe.net	187.16.216.121	42473	x	39073
rrc15.ripe.net	187.16.208.144	24482	x	39073
rrc15.ripe.net	187.16.209.243	271253	x	39073
rrc15.ripe.net	187.16.222.45	263237	x	39073
rrc15.ripe.net	187.16.217.161	13786	x	39073
rrc15.ripe.net	187.16.222.156	264479	x	39073
rrc15.ripe.net	187.16.213.225	6424	x	39073
rrc15.ripe.net	187.16.222.229	199524	x	39073
rrc15.ripe.net	187.16.220.159	917	x	39073
rrc15.ripe.net	187.16.217.110	23106	x	39073
rrc15.ripe.net	187.16.222.107	263152	x	39073
rrc16.ripe.net	198.32.243.133	199524	x	39073
rrc16.ripe.net	198.32.242.254	52320	x	39073
rrc16.ripe.net	198.32.242.55	20080	x	39073
rrc19.ripe.net	196.60.9.165	917	x	39073
rrc19.ripe.net	196.60.8.44	327983	x	39073
rrc19.ripe.net	196.60.8.139	32653	x	39073
rrc19.ripe.net	196.60.8.152	3491	x	39073
rrc19.ripe.net	196.60.9.84	37697	x	39073
rrc19.ripe.net	196.60.8.178	37271	x	39073
rrc19.ripe.net	196.60.8.221	327804	x	39073
rrc19.ripe.net	196.60.8.190	37239	x	39073
rrc19.ripe.net	196.60.9.188	199524	x	39073
rrc19.ripe.net	196.60.10.50	3257	x	39073

rrc19.ripe.net	196.60.8.22	327960	x	39073
rrc25.ripe.net	203.240.229.2	138195	x	39073
rrc25.ripe.net	185.255.53.202	3214	x	39073
rrc25.ripe.net	91.132.202.2	35710	x	39073
rrc25.ripe.net	193.28.236.32	30950	x	39073
rrc25.ripe.net	217.76.0.17	43733	x	39073
rrc25.ripe.net	77.243.32.3	31027	x	39073
rrc25.ripe.net	178.248.51.149	51185	x	39073
rrc25.ripe.net	66.255.243.37	13781	x	39073
rrc25.ripe.net	23.175.208.254	54316	x	39073
rrc25.ripe.net	185.121.168.42	924	x	39073
rrc25.ripe.net	94.207.42.2	57187	x	39073
rrc25.ripe.net	14.1.54.38	61138	x	39073
rrc25.ripe.net	103.74.171.30	132847	x	39073
rrc25.ripe.net	146.19.145.216	8888	x	39073
rrc25.ripe.net	192.154.3.129	394414	x	39073
rrc25.ripe.net	62.115.129.90	1299	x	39073
rrc25.ripe.net	45.67.83.250	207910	x	39073
rrc25.ripe.net	103.176.189.0	149794	x	39073
rrc25.ripe.net	130.244.51.154	1257	x	39073
rrc25.ripe.net	23.159.16.22	835	x	39073
rrc25.ripe.net	193.148.249.191	212123	x	39073
rrc25.ripe.net	157.15.254.68	151381	x	39073
rrc25.ripe.net	185.115.244.25	28824	x	39073
rrc25.ripe.net	103.87.125.0	45489	x	39073
rrc25.ripe.net	77.243.32.58	31027	x	39073

rrc25.ripe.net	46.245.142.4	197580	x	39073
rrc25.ripe.net	27.50.36.146	134823	x	39073
rrc25.ripe.net	154.18.4.110	134823	x	39073
rrc25.ripe.net	103.167.66.1	142271	x	39073
rrc25.ripe.net	193.107.13.3	47787	x	39073
rrc25.ripe.net	104.225.4.202	36236	x	39073
rrc25.ripe.net	45.136.222.0	208431	x	39073
rrc25.ripe.net	80.241.0.70	21282	x	39073
rrc25.ripe.net	186.211.216.32	14840	x	39073
rrc25.ripe.net	109.200.212.1	49544	x	39073
rrc25.ripe.net	93.190.135.253	6881	x	39073
rrc25.ripe.net	103.152.35.254	38008	x	39073
rrc25.ripe.net	176.119.210.1	56457	x	39073
rrc25.ripe.net	46.8.37.63	198150	x	39073
rrc25.ripe.net	194.28.99.120	34872	x	39073
rrc25.ripe.net	79.143.96.61	15397	x	39073
rrc25.ripe.net	31.15.255.209	3212	x	39073
rrc25.ripe.net	193.43.214.253	44097	x	39073
rrc25.ripe.net	195.69.189.4	28910	x	39073
rrc25.ripe.net	23.130.139.83	212934	x	39073
rrc25.ripe.net	152.89.170.250	212271	x	39073
route-views4	45.112.244.1	63956	x	39073
route-views4	103.96.117.253	133950	x	39073
route-views4	103.247.3.36	58511	x	39073
route-views4	103.247.3.143	58511	x	39073

route-views4	212.81.56.228	57050	x	39073
route-views4	104.225.4.202	36236	x	39073
route-views4	129.250.1.248	2914	x	39073
route-views4	192.43.217.142	14041	x	39073
route-views4	198.98.84.183	19754	x	39073
route-views4	109.233.180.32	34288	x	39073
route-views4	203.175.175.15	24482	x	39073
route-views4	212.81.56.227	57050	x	39073
route-views4	114.141.109.44	45437	x	39073
route-views4	133.205.1.142	2518	x	39073
route-views4	103.52.116.4	63956	x	39073
route-views4	132.198.255.254	1351	x	39073
route-views4	154.72.103.192	32653	x	39073
route-views4	193.28.236.32	30950	x	39073
route-views4	31.204.91.150	56665	x	39073
route-views4	119.18.185.44	38726	x	39073
rrc11.ripe.net	198.32.160.242	24482	x	39073
rrc11.ripe.net	198.32.160.137	19151	x	39073
rrc11.ripe.net	198.32.160.182	9002	x	39073
rrc11.ripe.net	198.32.160.42	2497	x	39073
rrc11.ripe.net	198.32.160.39	9304	x	39073
rrc11.ripe.net	198.32.160.103	13030	x	39073
rrc11.ripe.net	198.32.160.58	21700	x	39073
rrc11.ripe.net	198.32.160.12	199524	x	39073
rrc13.ripe.net	195.208.208.147	28917	x	39073
rrc13.ripe.net	195.208.209.109	24482	x	39073
rrc13.ripe.net	195.208.209.66	35598	x	39073
rrc13.ripe.net	195.208.210.52	41722	x	39073
rrc13.ripe.net	195.208.209.4	41095	x	39073
rrc13.ripe.net	195.208.208.223	20764	x	39073
route-views.chile	200.16.114.53	27678	x	39073

route-views.eqix	206.126.236.189	6057	x	39073
route-views.eqix	206.126.236.137	293	x	39073
route-views.eqix	206.126.237.210	49544	x	39073
route-views.eqix	206.126.236.47	19151	x	39073
route-views.eqix	206.126.238.209	17350	x	39073
route-views.eqix	206.126.238.64	8220	x	39073
route-views.eqix	206.126.236.12	2914	x	39073
route-views.eqix	206.126.236.19	3257	x	39073
route-views.eqix	206.126.236.172	11039	x	39073
route-views.eqix	206.126.236.120	41095	x	39073
route-views.eqix	206.126.238.92	16552	x	39073
route-views.eqix	206.126.237.22	199524	x	39073
route-views.eqix	206.126.236.25	6079	x	39073
route-views.eqix	206.126.236.37	6939	x	39073
route-views.eqix	206.126.236.214	57695	x	39073
route-views.eqix	206.126.236.117	6830	x	39073
route-views.eqix	206.126.238.208	17350	x	39073
route-views.eqix	206.126.236.209	398465	x	39073
route-views.linx	195.66.236.175	13030	x	39073
route-views.linx	195.66.225.196	41811	x	39073
route-views.linx	195.66.225.146	49544	x	39073
route-views.linx	195.66.224.21	6939	x	39073
route-views.linx	195.66.224.99	13237	x	39073
route-views.linx	195.66.224.25	328832	x	39073
route-views.linx	195.66.226.254	48070	x	39073
route-views.linx	195.66.225.86	34288	x	39073
route-views.linx	195.66.224.89	6830	x	39073
route-views.linx	195.66.236.114	6667	x	39073
route-views.linx	195.66.224.165	38880	x	39073

route-views.linx	195.66.226.97	39122	x	39073
route-views.linx	195.66.226.33	59605	x	39073
route-views.linx	195.66.224.114	6667	x	39073
route-views.linx	195.66.224.118	14537	x	39073
route-views.linx	195.66.226.102	37271	x	39073
route-views.linx	195.66.225.212	6424	x	39073
route-views.linx	195.66.227.118	8455	x	39073
route-views.linx	195.66.238.214	58511	x	39073
route-views.linx	195.66.224.51	6453	x	39073
route-views.linx	195.66.224.32	3257	x	39073
route-views.linx	195.66.226.39	267613	x	39073
route-views.linx	195.66.224.193	9002	x	39073
route-views.linx	195.66.227.195	3170	x	39073
route-views.linx	195.66.224.175	13030	x	39073
route-views.linx	195.66.224.138	2914	x	39073
route-views.linx	195.66.226.214	58511	x	39073
route-views.linx	195.66.227.122	398465	x	39073
route-views.linx	195.66.224.157	16552	x	39073
route-views.linx	195.66.224.167	3491	x	39073
route-views.amsix	80.249.212.84	42541	x	39073
route-views.amsix	80.249.208.50	1103	x	39073
route-views.amsix	80.249.209.17	12779	x	39073
route-views.amsix	80.249.209.216	9002	x	39073
route-views.amsix	80.249.208.152	39591	x	39073
route-views.amsix	185.1.167.149	200242	x	39073
route-views.amsix	80.249.213.223	267613	x	39073
route-views.amsix	80.249.214.44	16552	x	39073
route-views.amsix	80.249.208.209	51088	x	39073
route-views.amsix	80.249.208.106	6830	x	39073

route-views.amsix	80.249.212.75	38880	x	39073
route-views.amsix	185.1.167.118	8888	x	39073
route-views.amsix	80.249.208.35	12859	x	39073
route-views.amsix	80.249.210.150	199524	x	39073
route-views.amsix	185.1.167.56	216311	x	39073
route-views.amsix	185.1.166.237	213151	x	39073
route-views.amsix	80.249.212.104	58511	x	39073
route-views.amsix	80.249.212.156	3399	x	39073
route-views.flix	206.41.108.147	16552	x	39073
route-views.flix	206.41.108.110	52468	x	39073
route-views.flix	206.41.108.60	52320	x	39073
route-views.flix	206.41.108.150	52468	x	39073
route-views.flix	206.41.108.178	264409	x	39073
route-views.flix	206.41.108.23	6939	x	39073
route-views.flix	206.41.108.11	19151	x	39073
route-views.fortaleza	45.184.144.128	52320	x	39073
route-views.fortaleza	45.184.146.7	262462	x	39073
route-views.fortaleza	45.184.146.59	199524	x	39073
route-views.fortaleza	45.184.144.187	28624	x	39073
route-views.fortaleza	45.184.145.15	264479	x	39073
route-views.isc	198.32.176.20	6939	x	39073
route-views.isc	198.32.176.95	49544	x	39073
route-views.isc	198.32.176.226	199524	x	39073
route-views.isc	198.32.176.164	19151	x	39073
route-views.isc	198.32.176.177	7575	x	39073
route-views.kixp	196.223.21.73	37271	x	39073

route-views.kixp	196.223.21.74	6939	x	39073
route-views.kixp	196.223.21.72	37271	x	39073
collector14.bgp.he.net	172.18.14.1	6939	x	39073
collector14.bgp.he.net	172.18.14.2	6939	x	39073
route-views.chicago	208.115.137.200	14630	x	39073
route-views.chicago	208.115.136.18	19151	x	39073
route-views.chicago	208.115.136.95	17350	x	39073
route-views.chicago	208.115.136.58	293	x	39073
route-views.chicago	208.115.136.67	852	x	39073
route-views.chicago	208.115.136.134	32709	x	39073
route-views.chicago	208.115.136.5	17350	x	39073
route-views.chicago	208.115.137.69	16552	x	39073
route-views.chicago	208.115.137.47	398465	x	39073
route-views.chicago	208.115.136.133	19653	x	39073
route-views.chicago	208.115.137.50	49544	x	39073
route-views.chicago	208.115.137.100	14630	x	39073
route-views.chicago	208.115.136.220	53828	x	39073
route-views.chicago	208.115.136.42	199524	x	39073
route-views.chicago	208.115.137.35	8220	x	39073
route-views2.saopaulo	187.16.209.34	271253	x	39073
route-views2.saopaulo	187.16.219.247	263541	x	39073
route-views2.saopaulo	187.16.222.16	199524	x	39073
route-views2.saopaulo	187.16.222.221	263009	x	39073
route-views2.saopaulo	187.16.219.29	16552	x	39073
route-views2.saopaulo	187.16.218.138	268976	x	39073

route-views2.saopaulo	187.16.220.229	49544	x	39073
route-views2.saopaulo	187.16.214.101	53427	x	39073
route-views2.saopaulo	187.16.219.20	61832	x	39073
route-views2.saopaulo	187.16.215.63	264409	x	39073
route-views2.saopaulo	187.16.222.156	264479	x	39073
route-views2.saopaulo	187.16.222.229	199524	x	39073
route-views2.saopaulo	187.16.222.168	262791	x	39073
route-views2.saopaulo	187.16.221.193	37468	x	39073
route-views2.saopaulo	187.16.209.243	271253	x	39073
route-views2.saopaulo	187.16.217.27	28329	x	39073
route-views2.saopaulo	187.16.220.216	52873	x	39073
route-views2.saopaulo	187.16.216.232	28329	x	39073
route-views.napafrica	196.60.8.113	328512	x	39073
route-views.napafrica	196.60.10.62	16552	x	39073
route-views.napafrica	196.60.8.152	3491	x	39073
route-views.napafrica	196.60.8.60	37468	x	39073
route-views.napafrica	196.60.8.142	37271	x	39073
route-views.napafrica	196.60.9.139	32653	x	39073
route-views.napafrica	196.60.10.195	328964	x	39073
route-views.napafrica	196.60.8.6	49544	x	39073
route-views.napafrica	196.60.8.178	37271	x	39073
route-views.napafrica	196.60.10.232	328964	x	39073

route-views.napafrica	196.60.10.50	3257	x	39073
route-views.napafrica	196.60.8.139	32653	x	39073
route-views.napafrica	196.60.9.188	199524	x	39073
route-views.soxrs	185.1.27.32	199524	x	39073
route-views.phoix	198.32.172.171	150000	x	39073
route-views.sydney	45.127.172.74	4826	x	39073
route-views.sydney	45.127.172.80	3491	x	39073
route-views.sydney	45.127.172.152	132847	x	39073
route-views.sydney	45.127.172.196	24516	x	39073
route-views.sydney	45.127.172.78	199524	x	39073
route-views.sydney	45.127.173.20	8888	x	39073
route-views.sydney	45.127.173.76	398465	x	39073
route-views.sydney	45.127.173.77	3257	x	39073
route-views.sydney	45.127.173.40	135895	x	39073
route-views.sydney	45.127.173.66	7594	x	39073
route-views.sydney	45.127.173.71	16552	x	39073
route-views.sydney	45.127.172.46	7575	x	39073
route-views.sydney	45.127.172.67	148968	x	39073
route-views.sydney	45.127.172.149	58511	x	39073
route-views.uaeix	185.1.8.114	199524	x	39073
route-views.uaeix	185.1.8.11	42473	x	39073
route-views.uaeix	185.1.8.59	49544	x	39073
route-views.uaeix	185.1.8.23	60924	x	39073
pit.scl	45.68.16.3	64112	x	39073
route-views	89.149.178.10	3257	x	39073

route-views	208.51.134.246	3549	x	39073
route-views	208.51.134.255	3549	x	39073
route-views	77.39.192.30	20912	x	39073
route-views	147.28.7.2	3130	x	39073
route-views	91.218.184.60	49788	x	39073
route-views	129.250.1.71	2914	x	39073
route-views	140.192.8.16	20130	x	39073
route-views	168.209.255.56	3741	x	39073
route-views	94.156.252.18	34224	x	39073
route-views	37.139.139.17	57866	x	39073
route-views	105.16.0.247	37100	x	39073
route-views	12.0.1.63	7018	x	39073
route-views	217.192.89.50	3303	x	39073
route-views	45.61.0.85	22652	x	39073
route-views	64.71.137.241	6939	x	39073
route-views	202.73.40.45	18106	x	39073
route-views	202.232.0.3	2497	x	39073
route-views	206.24.210.80	3561	x	39073
route-views	137.164.16.84	2152	x	39073
route-views	198.58.198.252	1403	x	39073
route-views	198.129.33.85	293	x	39073
route-views.sg	27.111.229.225	49544	x	39073
route-views.sg	27.111.228.77	7713	x	39073
route-views.sg	27.111.228.155	7713	x	39073
route-views.sg	27.111.228.217	3257	x	39073
route-views.sg	27.111.229.103	9002	x	39073
route-views.sg	27.111.228.159	24482	x	39073
route-views.sg	27.111.228.127	17660	x	39073
route-views.sg	27.111.229.175	58511	x	39073
route-views.sg	27.111.229.252	16552	x	39073
route-views.sg	27.111.228.134	132337	x	39073

route-views.sg	27.111.228.6	18106	x	39073
route-views.sg	27.111.228.222	199524	x	39073
route-views.sg	27.111.228.43	3491	x	39073
route-views.sg	27.111.229.123	8220	x	39073
route-views.perth	218.100.76.80	136557	x	39073
route-views.perth	218.100.78.35	58511	x	39073
route-views.perth	218.100.52.60	49544	x	39073
route-views.perth	218.100.76.5	7594	x	39073
route-views.perth	218.100.78.46	140627	x	39073
route-views.perth	218.100.52.219	199524	x	39073
route-views.perth	218.100.76.10	58511	x	39073
route-views.perth	27.106.192.5	58511	x	39073
route-views.perth	218.100.52.56	58511	x	39073
route-views.perth	218.100.78.98	136557	x	39073
route-views.perth	218.100.52.247	136557	x	39073
route-views.perth	218.100.76.17	140627	x	39073
route-views.rio	45.6.54.171	199524	x	39073
route-views.rio	45.6.54.203	6057	x	39073
route-views.rio	45.6.52.62	267613	x	39073
route-views.rio	45.6.54.199	999	x	39073
route-views.rio	45.6.55.32	52468	x	39073
route-views.rio	45.6.52.193	52320	x	39073
route-views.rio	45.6.53.167	264479	x	39073
route-views.sfmix	206.197.187.41	35008	x	39073
route-views.sfmix	206.197.187.51	64289	x	39073

route-views.sfmix	206.197.187.87	49544	x	39073
route-views.sfmix	206.197.187.106	34927	x	39073
route-views.sfmix	206.197.187.85	397131	x	39073
route-views.telxatl	206.126.110.155	53828	x	39073
route-views.telxatl	206.126.110.28	4181	x	39073
route-views.telxatl	206.126.110.152	6082	x	39073
route-views.telxatl	206.126.110.75	6939	x	39073
route-views.telxatl	206.126.110.12	19151	x	39073
decix.jhb	103.162.254.114	199524	x	39073
route-views.nwax	198.32.195.30	6423	x	39073
route-views.wide	202.249.2.83	n/a	x	39073
route-views.wide	202.249.2.169	2497	x	39073
route-views.wide	202.249.2.86	7500	x	39073
route-views.ny	206.82.104.251	64289	x	39073
route-views.ny	206.82.104.185	398465	x	39073
route-views.ny	206.82.104.63	49544	x	39073
route-views.ny	206.82.104.161	11399	x	39073
route-views3	64.71.137.241	6939	x	39073
route-views3	162.211.99.255	55222	x	39073
route-views3	195.239.252.124	3216	x	39073
route-views3	205.171.3.54	209	x	39073
route-views3	158.106.197.135	46450	x	39073
route-views3	206.198.182.15	23367	x	39073
route-views3	67.219.192.5	19653	x	39073
route-views3	89.21.210.85	39120	x	39073
route-views3	195.239.77.236	3216	x	39073
route-views3	202.150.221.33	38001	x	39073
route-views3	72.36.126.8	40387	x	39073
route-views3	208.94.118.10	40630	x	39073

route-views3	94.101.60.146	39120	x	39073
route-views3	109.233.62.1	29479	x	39073
route-views3	210.5.41.225	45352	x	39073
route-views3	89.149.178.10	3257	x	39073
route-views3	203.62.187.103	9268	x	39073
route-views3	5.157.4.250	8289	x	39073
route-views3	43.226.4.1	63927	x	39073
route-views3	203.62.187.102	9268	x	39073
route-views3	64.250.124.15	23367	x	39073
route-views3	205.171.8.123	209	x	39073
route-views3	206.248.155.130	5645	x	39073
route-views3	190.15.124.18	61568	x	39073
route-views3	205.171.200.245	209	x	39073
route-views3	206.24.210.80	3561	x	39073
route-views3	104.251.122.1	14315	x	39073
route-views3	89.21.210.86	39120	x	39073
rrc01.ripe.net	5.57.81.76	36924	x	39073
rrc01.ripe.net	195.66.224.167	3491	x	39073
rrc01.ripe.net	195.66.224.137	3320	x	39073
rrc01.ripe.net	195.66.224.81	1828	x	39073
rrc01.ripe.net	5.57.81.127	48070	x	39073
rrc01.ripe.net	195.66.226.113	42473	x	39073
rrc01.ripe.net	195.66.224.138	2914	x	39073
rrc01.ripe.net	5.57.81.21	6908	x	39073
rrc01.ripe.net	195.66.231.56	271253	x	39073
rrc01.ripe.net	5.57.81.210	31742	x	39073
rrc01.ripe.net	195.66.224.193	9002	x	39073
rrc01.ripe.net	195.66.226.232	12969	x	39073
rrc01.ripe.net	195.66.226.13	8896	x	39073
rrc01.ripe.net	195.66.225.32	6908	x	39073
rrc01.ripe.net	195.66.227.233	20784	x	39073

		1		
rrc01.ripe.net	195.66.227.195	3170	x	39073
rrc01.ripe.net	195.66.227.163	1299	x	39073
rrc01.ripe.net	5.57.81.231	917	x	39073
rrc01.ripe.net	195.66.227.148	14630	x	39073
rrc01.ripe.net	195.66.226.97	39122	x	39073
rrc01.ripe.net	195.66.224.175	13030	x	39073
rrc01.ripe.net	195.66.226.31	12779	x	39073
rrc01.ripe.net	195.66.224.76	6461	x	39073
rrc01.ripe.net	195.66.224.89	6830	x	39073
rrc01.ripe.net	195.66.227.193	6233	x	39073
rrc01.ripe.net	195.66.227.105	34927	x	39073
rrc01.ripe.net	5.57.81.186	6894	x	39073
rrc01.ripe.net	195.66.225.48	62167	x	39073
rrc01.ripe.net	5.57.81.216	35266	x	39073
rrc01.ripe.net	195.66.225.216	25160	x	39073
rrc01.ripe.net	195.66.225.212	6424	x	39073
rrc01.ripe.net	195.66.226.38	24482	x	39073
rrc01.ripe.net	195.66.224.32	3257	x	39073
rrc01.ripe.net	5.57.80.210	8218	x	39073
rrc01.ripe.net	195.66.224.26	396998	x	39073
rrc12.ripe.net	80.81.193.18	24482	x	39073
rrc12.ripe.net	80.81.195.166	47147	x	39073
rrc12.ripe.net	80.81.193.65	51184	x	39073
rrc12.ripe.net	80.81.192.46	2914	x	39073
rrc12.ripe.net	80.81.193.145	34019	x	39073
rrc12.ripe.net	80.81.194.119	34288	x	39073
rrc12.ripe.net	80.81.195.35	35710	x	39073
rrc12.ripe.net	80.81.193.139	48362	x	39073
rrc12.ripe.net	80.81.197.27	210937	x	39073

rrc12.ripe.net	80.81.194.100	47692	x	39073
rrc12.ripe.net	80.81.193.194	48919	x	39073
rrc12.ripe.net	80.81.194.45	205112	x	39073
rrc12.ripe.net	80.81.192.194	6762	x	39073
rrc12.ripe.net	80.81.195.225	48821	x	39073
rrc12.ripe.net	80.81.195.219	58057	x	39073
rrc12.ripe.net	80.81.192.231	57695	x	39073
rrc12.ripe.net	80.81.193.247	35598	x	39073
rrc12.ripe.net	80.81.192.222	680	x	39073
rrc12.ripe.net	80.81.195.98	6233	x	39073
rrc12.ripe.net	80.81.194.140	25220	x	39073
rrc12.ripe.net	80.81.196.197	58299	x	39073
rrc12.ripe.net	80.81.196.225	213151	x	39073
rrc12.ripe.net	80.81.195.171	64475	x	39073
rrc12.ripe.net	80.81.193.252	199524	x	39073
rrc12.ripe.net	80.81.194.186	12779	x	39073
rrc12.ripe.net	80.81.196.156	34927	x	39073
rrc12.ripe.net	80.81.194.240	50629	x	39073
rrc12.ripe.net	80.81.196.110	3257	x	39073
rrc12.ripe.net	80.81.192.13	8218	x	39073
rrc12.ripe.net	80.81.194.59	29140	x	39073
rrc12.ripe.net	80.81.192.162	24961	x	39073
rrc12.ripe.net	80.81.196.189	21412	x	39073
rrc12.ripe.net	80.81.194.26	6461	x	39073
rrc12.ripe.net	80.81.192.175	553	x	39073
rrc12.ripe.net	80.81.195.178	206356	x	39073
rrc07.ripe.net	194.68.123.57	3399	x	39073
rrc07.ripe.net	194.68.123.96	35280	x	39073
rrc07.ripe.net	194.68.123.136	6667	x	39073

rrc07.ripe.net	194.68.123.226	24482	x	39073
rrc07.ripe.net	194.68.123.157	9002	x	39073
rrc07.ripe.net	194.68.123.18	42473	x	39073
rrc07.ripe.net	194.68.123.69	51519	x	39073
rrc07.ripe.net	194.68.123.191	199524	x	39073
rrc10.ripe.net	217.29.66.127	49605	x	39073
rrc10.ripe.net	217.29.66.233	8660	x	39073
rrc10.ripe.net	217.29.67.55	199524	x	39073
rrc10.ripe.net	217.29.67.54	20912	x	39073
rrc10.ripe.net	217.29.67.51	41327	x	39073
rrc10.ripe.net	217.29.66.225	50877	x	39073
rrc10.ripe.net	217.29.66.102	51185	x	39073
rrc10.ripe.net	217.29.66.88	20811	x	39073
rrc10.ripe.net	217.29.66.120	15605	x	39073
rrc10.ripe.net	217.29.66.5	5392	x	39073
rrc10.ripe.net	217.29.66.65	12779	x	39073
rrc10.ripe.net	217.29.67.13	57111	x	39073
rrc10.ripe.net	217.29.66.158	24482	x	39073
rrc10.ripe.net	217.29.66.86	12637	x	39073
rrc18.ripe.net	193.242.98.141	29680	x	39073
rrc20.ripe.net	91.206.52.127	20612	x	39073
rrc20.ripe.net	91.206.52.109	198385	x	39073
rrc20.ripe.net	91.206.52.115	6461	x	39073
rrc20.ripe.net	91.206.52.9	29691	x	39073
rrc20.ripe.net	91.206.52.68	12307	x	39073
rrc20.ripe.net	91.206.52.32	21232	x	39073
rrc20.ripe.net	91.206.52.103	196621	x	39073
rrc20.ripe.net	91.206.52.180	62167	x	39073
rrc20.ripe.net	91.206.53.12	8298	x	39073

rrc20.ripe.net	91.206.52.141	59891	x	39073
rrc20.ripe.net	91.206.53.35	57777	x	39073
rrc20.ripe.net	91.206.52.116	8218	x	39073
rrc20.ripe.net	91.206.52.40	48362	x	39073
rrc20.ripe.net	91.206.52.126	20612	x	39073
rrc20.ripe.net	91.206.52.236	34927	x	39073
rrc20.ripe.net	91.206.52.205	24482	x	39073
rrc20.ripe.net	91.206.52.246	51786	x	39073
rrc20.ripe.net	91.206.52.90	59414	x	39073
rrc20.ripe.net	91.206.52.5	47147	x	39073
rrc20.ripe.net	91.206.52.117	25091	x	39073
rrc20.ripe.net	2001:7f8:24::b1	58057	x	39073
rrc20.ripe.net	91.206.52.6	8758	x	39073
rrc20.ripe.net	91.206.52.15	15623	x	39073
rrc20.ripe.net	91.206.52.197	51873	x	39073
rrc21.ripe.net	37.49.237.180	6461	x	39073
rrc21.ripe.net	37.49.236.61	8426	x	39073
rrc21.ripe.net	37.49.236.156	15547	x	39073
rrc21.ripe.net	37.49.236.249	49434	x	39073
rrc21.ripe.net	37.49.236.246	2613	x	39073
rrc21.ripe.net	37.49.237.231	35426	x	39073
rrc21.ripe.net	37.49.237.83	25091	x	39073
rrc21.ripe.net	37.49.237.175	199524	x	39073
rrc21.ripe.net	37.49.236.177	12779	x	39073
rrc21.ripe.net	37.49.236.71	34019	x	39073
rrc21.ripe.net	37.49.236.55	35600	x	39073
rrc21.ripe.net	37.49.236.27	2027	x	39073
rrc21.ripe.net	37.49.236.32	34177	x	39073
rrc21.ripe.net	37.49.236.1	8218	x	39073
rrc21.ripe.net	37.49.237.143	50628	x	39073
rrc21.ripe.net	37.49.236.172	58308	x	39073

rrc21.ripe.net	37.49.232.11	14907	x	39073
rrc21.ripe.net	37.49.236.205	29075	x	39073
rrc21.ripe.net	37.49.232.7	8218	x	39073
rrc21.ripe.net	37.49.236.228	24482	x	39073
rrc22.ripe.net	86.104.125.81	31554	x	39073
rrc22.ripe.net	86.104.125.59	56430	x	39073
rrc23.ripe.net	27.111.228.186	14907	x	39073
rrc23.ripe.net	27.111.228.217	3257	x	39073
rrc23.ripe.net	27.111.228.6	18106	x	39073
rrc23.ripe.net	27.111.229.103	9002	x	39073
rrc23.ripe.net	27.111.228.222	199524	x	39073
rrc23.ripe.net	27.111.228.43	3491	x	39073
rrc23.ripe.net	27.111.228.218	396998	x	39073
rrc23.ripe.net	27.111.230.35	133210	x	39073
rrc23.ripe.net	27.111.229.245	35280	x	39073
rrc23.ripe.net	27.111.229.225	49544	x	39073
rrc24.ripe.net	200.40.162.202	6057	x	39073
rrc24.ripe.net	45.65.244.1	265721	x	39073
rrc24.ripe.net	185.197.26.1	49544	x	39073
rrc24.ripe.net	5.188.4.211	46997	x	39073
rrc24.ripe.net	190.112.55.254	264845	x	39073
rrc24.ripe.net	138.122.60.1	61573	x	39073
rrc24.ripe.net	185.197.24.1	49544	x	39073
rrc24.ripe.net	186.211.184.34	14840	x	39073
rrc24.ripe.net	168.195.131.1	263702	x	39073
rrc24.ripe.net	186.211.136.32	14840	x	39073
rrc24.ripe.net	186.211.128.34	14840	x	39073

rrc26.ripe.net	185.1.8.59	49544	x	39073
rrc26.ripe.net	185.1.8.3	48237	x	39073
rrc26.ripe.net	185.1.8.50	200612	x	39073
route-views5	65.19.141.130	199518	x	39073
route-views5	103.247.3.36	58511	x	39073
route-views5	170.39.196.254	33185	x	39073
route-views5	23.155.8.1	22296	x	39073
route-views5	185.197.24.1	49544	x	39073
route-views5	185.197.26.1	49544	x	39073
route-views5	188.122.95.61	49544	x	39073
route-views5	203.62.252.92	1221	x	39073
route-views5	45.94.151.1	208594	x	39073
route-views5	91.216.79.0	41666	x	39073
route-views5	103.26.244.151	132884	x	39073
route-views5	103.203.242.1	955	x	39073
route-views5	192.108.73.66	13058	x	39073
route-views5	5.180.58.0	56987	x	39073
route-views5	66.118.229.23	955	x	39073
route-views5	193.148.248.178	60539	x	39073
route-views5	103.247.3.142	58511	x	39073
route-views5	202.165.70.255	137409	x	39073
route-views5	207.2.124.0	19529	x	39073
route-views5	185.156.96.227	207934	x	39073

That’s for every facility in the Russian Federation. Those are live-feed supervisory control direct connections from the UES Grid Network Operations Center (gNOC) to the individual electrical facilities, power plants, electrical substations and UES branch offices. From the gNOC control room the entire Russian electrical system is monitored and managed 24/7 and can perform any task as if they were on-site. The System

Operator of the Unified Energy System (SO UES) in Russia uses an automated monitoring and control system known as the Automated Dispatch Control System (ADCS). This system provides real-time data feeds and management of all aspects of the electrical grid, including power generation, transmission, and distribution.

The ADCS integrates data from various regional dispatch centers, substations, and power plants, enabling centralized control over Russia's vast power network. It allows operators to monitor the status of the grid in real time, manage the load balance, and respond quickly to any disruptions or emergencies.

Additionally, SO UES also employs advanced Supervisory Control and Data Acquisition (SCADA) systems to further enhance monitoring and remote control capabilities. These systems are designed to collect data from sensors across the grid infrastructure, helping operators forecast power demand, prevent overloads, and optimize energy distribution. These systems, together with forecasting tools and digital models of the grid, enable SO UES to manage the vast complexity of Russia's power network effectively.

The SO UES centalized National Grid Systems Network Operations Center is a physical link to the underlying energy infrastructure but it does not currently have the capabilities of AI-based management on it’s own host platform, for that the UES gNOC is mirrored to the Directorate of Emergency Situations in the Ministry of Civil Defense, Emergencies and Disaster Relief which is a state agency overseeing the civil emergency services in Russia and established the Russian Rescue Corps and assigned it the mission of rapid response to emergencies, including power transmission, generation and delivery of electricity during emergencies which is located in the The National Defense Management Center, also known as the National Defense Control Center (NDCC), formerly the Central Command Post of the General Staff of the Russian Armed Forces is the supreme command and control center of the Russian Ministry of Defense and the Russian Armed Forces. The MoD Astra-Linux super computer provides the AI-based forecasting.

Astra-Linux is a Russian Linux-based computer operating system (OS) that is being widely deployed in the Russian Federation to replace Microsoft Windows. Initially it was created and developed to meet the needs of the Russian army, and other armed forces and intelligence agencies. It provides data protection up to the level of "top secret" in Russian information classification grade by featuring mandatory access control. It has been officially certified by Russian Defense Ministry, Federal Service for Technical and Export Control and Federal Security Service (FSB). Astra-Linux is the operating system language of the Russian state super-computer. In the course of 2010s, as Russian authorities and industry were trying to lower dependence on Western products ("import substitution industrialization"). Aside from army and police, it has now being supplied to educational, healthcare and other state institutions, as well as in

industry giants such as RZD, Gazprom, Rosatom and others. Server versions of Astra-Linux are certified to work with Huawei equipment.

The creator of the Astra-Linux OS is the Scientific/Manufacturing Enterprise Rusbitech which is applying solutions according to Russian Government decree No. 2299-p of 17 October 2010 that orders federal authorities and budget institutions to implement Free Software use. There are two available editions of the OS: the main one is called "Special Edition" and the other one is called "Common Edition". The main differences between the two are the fact that the former is paid, while the latter is free; the former is available for x86-64 architecture, ARM architecture and Elbrus architecture, while the latter is only available for x86-64 architecture; the former has a security certification and provides 3 levels of OS security (which are named after Russian cities and which from the lowest to the highest are: *Oryol*, *Voronezh* and *Smolensk*), while the latter doesn't have the security certification and only provides the lowest level of OS security (*Oryol*).

Rusbitech also manufactures a "soft/hardware trusted boot control module" MAKSIM-M1 ("M643M1") with PCI bus. It prevents unauthorized access and offers some other raised digital security features. The module, besides Astra Linux, also supports OSes with Linux kernel 2.6.x up to 5.x.x, as well as several Microsoft Windows OSes.[10]

The system uses .deb packages.

(image: Astra Linux Special Edition is being used in the Russian National Center for Defence Control)

Astra Linux is a recognized Debian derivative. Rusbitech has partnership relations with The Linux Foundation. It was part of the advisory board of The Document Foundation, but was suspended on 26 February 2022 because of the Russian invasion of Ukraine.

The Special Edition version (paid) is used in many Russian state-related organizations. Particularly, it is used in the Russian National Center for Defense Control (National Defense Management Center).

There are talks to deploy mass use of Astra Linux in many state institutions of the Republic of Crimea – legitimate use of other popular OSes is questionable because of international sanctions during the Russo-Ukrainian War. Also there were plans on cooperation of Rusbitech and Huawei. In January 2018, it was announced that Astra Linux was going to be deployed to all Russian Army computers, and Microsoft Windows will be dropped. In February 2018, Rusbitech announced it has ported Astra Linux to Russian-made Elbrus microprocessors.

In February 2019, Astra-Linux was announced to be implemented at Tianwan Nuclear Power Plant in China. Since 2019 "super-protected" tablet computers branded *MIG* are available with Astra Linux, smartphones are expected. In 2019 Gazprom national gas/oil holding announced Astra Linux implementation, in 2020 nuclear corporation Rosatom, in early 2021 Russian Railways was reported to do so. In 2020, Astra Linux sold more than a million copies in licenses and generated 2 billion rubles in sales. In 2021, several Russian nuclear power plants and subsidiaries of Rosatom are planned to switch to Astra Linux, with a total of 15000 users In July 2022 after Microsoft had decided to exit the Russian market, Astra-Linux announced that it was planning to be publicly listed on the Moscow Exchange, although it did not supply a date for the planned listing at the time.

Starting with the x.7 update, the *Astra Linux Special Edition* operating system uses a nested package repository structure – and this structure comprises the main repository, the base repository, and the extended repository.The main x.7 repository is generally identical to version 1.6 – and the base repository encompasses all core packages, as well as packages related to development tools.

The extended repository houses versions of software packages that are not found in the primary and base repositories. Such software operates within the Astra- Linux environment, remains unaltered to incorporate security features with CSS, may not be compatible with packages from the base and main repositories, and does not undergo certification tests.

The extended repository offers more functionality than a basic and core repository, with extended repository packages capable of modifying basic packages but not core packages. Additionally, the extended repository includes a backport's component that supplies the latest versions of packages that might not be compatible with packages from the basic and extended repositories, and an "*Astra-ce* component" that furnishes packages to ensure maximum compatibility with third-party software.

Using an extended repository enables users to install and run software originally designed for other Linux systems, develop their own software, and adapt Astra-Linux to various hardware platforms.

The primary categories of extended repository software packages are packages not included in the base repository, packages that update the base repository (i.e., newer versions of the basic repository packages – if incompatible, they are integrated into the backports component), and packages that substitute packages from the main repository. The latter are consolidated in the *Astra-ce* component, which includes: PostgreSQL DBMS, Exim (*Exim4*) email service, MariaDB DBMS packages, Java OpenJDK tools, and LibreOffice office suites.

Versions of Astra-Linux Special Edition

Version	Release date	Linux kernel
1.2	28 October 2011	2.6.34
1.3	26 April 2013	3.2.0
1.4	19 December 2014	3.16.0
1.5	8 April 2016	4.2.0
1.6	12 October 2018	4.15.0
1.7	22 October 2021	5.4
1.7.3	29 November 2022	5.15
1.7.5	16 October 2023	6.1
1.8	1 August 2024	6.6 or 6.1 LTS

Versions of Astra-Linux Common Edition

Version	Release date	Linux kernel
1.5	ending of 2009	2.6.31
1.6	23 November 2010	—
1.7	3 February 2012	2.6.34
1.9	12 February 2013	3.2.0
1.10	14 November 2014	3.16.0
1.11	17 March 2016	4.2.0
2.12	21 August 2018	4.15
2.12.29	14 May 2020	4.15.3-2
2.12.40	29 December 2020	5.4
2.12.43	8 September 2021	5.10
2.12.45	4 August 2022	5.15

NDMC Supercomputer is a military supercomputer with a speed of 16 petaflops. It is located in Moscow, Russia. The storage capacity is 236 petabytes.The supercomputer is designed to predict the development of armed conflicts and is able to analyze the situation and draw conclusions based on the information about past military conflicts. The database of the supercomputer contains data on the major armed conflicts of modernity for the efficient analysis of future threats and includes the SO UES energy balancing, monitoring and supervisory control of the Russian energy grid to autonomously manage the Russian electrical grid from the National Defense Management Center.

So now we know the organizational and hierarchical nomenclature of the Russian energy pool management infrastructure we see that the 655 real-time live C2 feeds all come together at the MSK-IX Moscow data center, server farm and platform interface whereby the Astra-Linux special edition AI-based intelligent intellect algorithms are trained in real time using Windows legacy live training and testing data from every available source

Pipedream is a software framework for malicious code targeting programmable logic controllers (PLCs) and industrial control systems (ICS), like SCADA HMI. First publicly disclosed in 2022, it has been described as a "Swiss Army knife" for hacking. It is believed to have been developed by Russian state-level Advanced Persistent Threat actors.
The name "Pipedream" was given by the cybersecurity company Dragos; the cybersecurity company Mandiant uses the name "Incontroller". It has been compared with the Industroyer toolkit used in the December 2015 Ukraine power grid cyberattack. Dragos refers to the authors of the software as Chernovite.

The toolkit consists of custom-made tools that, once they have established initial access in an operational technology (OT) network, enables them to scan for, compromise, and control certain ICS/SCADA devices, including the following:

Schneider Electric PLCs,
OMRON Sysmac NEX PLCs, and
Open Platform Communications Unified Architecture (OPC UA) servers.
Siemens HiMatic J7

The toolkit has a modular architecture and enables cyber actors to conduct highly automated exploits against targeted devices. The tools have a virtual console with a command interface that mirrors the interface of the targeted ICS/SCADA device. Modules interact with targeted devices, enabling operations by lower-skilled cyber actors to emulate higher-skilled actor capabilities.

APT actors can leverage the modules to scan for targeted devices, conduct reconnaissance on device details, upload malicious configuration/code to the targeted device, back up or restore device contents, and modify device parameters.

In addition, the APT actors can use a tool that installs and exploits a known-vulnerable ASRock-signed motherboard driver, AsrDrv103.sys, exploiting CVE-2020-15368 to execute malicious code in the Windows kernel. Successful deployment of this tool can allow APT actors to move laterally within an IT or OT environment and disrupt critical devices or functions.

Malware designed to target industrial control systems like power grids, factories, water utilities, and oil refineries represents a rare species of digital badness. So when the United States government warns of a piece of code built to target not just one of those industries, but potentially all of them, critical infrastructure owners worldwide should take notice.

The Department of Energy, the Cybersecurity and Infrastructure Security Agency, the NSA, and the FBI jointly released an advisory about a new hacker

toolset potentially capable of meddling with a wide range of industrial control system equipment. More than any previous industrial control system hacking toolkit, the malware contains an array of components designed to disrupt or take control of the functioning of devices, including programmable logic controllers (PLCs) that are sold by Schneider Electric and OMRON and are designed to serve as the interface between traditional computers and the actuators and sensors in industrial environments. Another component of the malware is designed to target Open Platform Communications Unified Architecture (OPC UA) servers—the computers that communicate with those controllers (Shodan search returned 618 OPC UA servers).

"This is the most expansive industrial control system attack tool that anyone has ever documented," says Sergio Caltagirone, the vice president of threat intelligence at industrial-focused cybersecurity firm Dragos, which contributed research to the advisory and published its own report about the malware. Researchers at Mandiant, Palo Alto Networks, Microsoft, and Schneider Electric also contributed to the advisory. “It’s like a Swiss Army knife with a huge number of pieces to it.”

Dragos says the malware has the ability to hijack target devices, disrupt or prevent operators from accessing them, permanently brick them, or even use them as a foothold to give hackers access to other parts of an industrial control system network. He notes that while the toolkit, which Dragos calls “Pipedream,” appears to specifically target Schneider Electric and OMRON PLCs, it does so by exploiting underlying software in those PLCs known as Codesys, which is used far more broadly across hundreds of other types of PLCs. This means that the malware could easily be adapted to work in almost any industrial environment. “This toolset is so big that it’s basically a free-for-all,” Caltagirone says. “There’s enough in here for everyone to worry about.”

The CISA advisory refers to an unnamed “APT actor” that developed the malware toolkit, using the common acronym APT to mean advanced persistent threat, a term for state-sponsored hacker groups. It's far from clear where the government agencies found the malware, or which country's hackers created it—though the timing of the advisory follows warnings from the Biden administration about the Russian government making preparatory moves to carry out disruptive cyberattacks in the midst of its invasion of Ukraine.

Dragos also declined to comment on the malware's origin. But Caltagirone says it doesn't appear to have been actually used against a victim—or at least, it hasn't yet triggered actual physical effects on a victim's industrial control systems. “We have high confidence it hasn’t been deployed yet for disruptive or destructive effects,” says Caltagirone.

While the toolkit's adaptability means it could be used against practically any industrial environment, from manufacturing to water treatment, Dragos points out that the apparent focus on Schneider Electric and OMRON PLCs does suggest that the hackers may have built it with power grid and oil refineries—particularly liquified natural gas facilities—in mind, given Schneider's wide use in electric utilities and OMRON's broad adoption in the oil and gas sector. Caltagirone suggests the ability to send commands to servo motors in those petrochemical facilities via OMRON PLCs would be particularly dangerous, with the ability to cause “destruction or even loss of life.”

The CISA advisory doesn't point to any particular vulnerabilities in the devices or software the Pipedream malware targets, though Caltagirone says it does exploit multiple zero-day vulnerabilities—previously unpatched hackable software flaws—that are still being fixed. He notes, however, that even patching those vulnerabilities won't prevent most of Pipedream's capabilities, as it's largely designed to hijack the intended functionality of target devices and send legitimate commands in the protocols they use. The CISA advisory includes a list of measures that infrastructure operators should take

to protect their operations, from limiting industrial control systems' network connections to implementing monitoring systems for ICS systems, in particular, that send alerts for suspicious behavior.

When WIRED reached out to Schneider Electric and OMRON, a Schneider spokesperson responded in a statement that the company has closely collaborated with the US government and security firm Mandiant and that they together "identified and developed protective measures to defend against" the newly revealed attack toolkit. "This is an instance of successful collaboration to deter threats on critical infrastructure before they occur and further underscores how public-private partnerships are instrumental to proactively detect and counter threats before they can be deployed," the company added. OMRON didn't immediately respond to WIRED's request for comment.

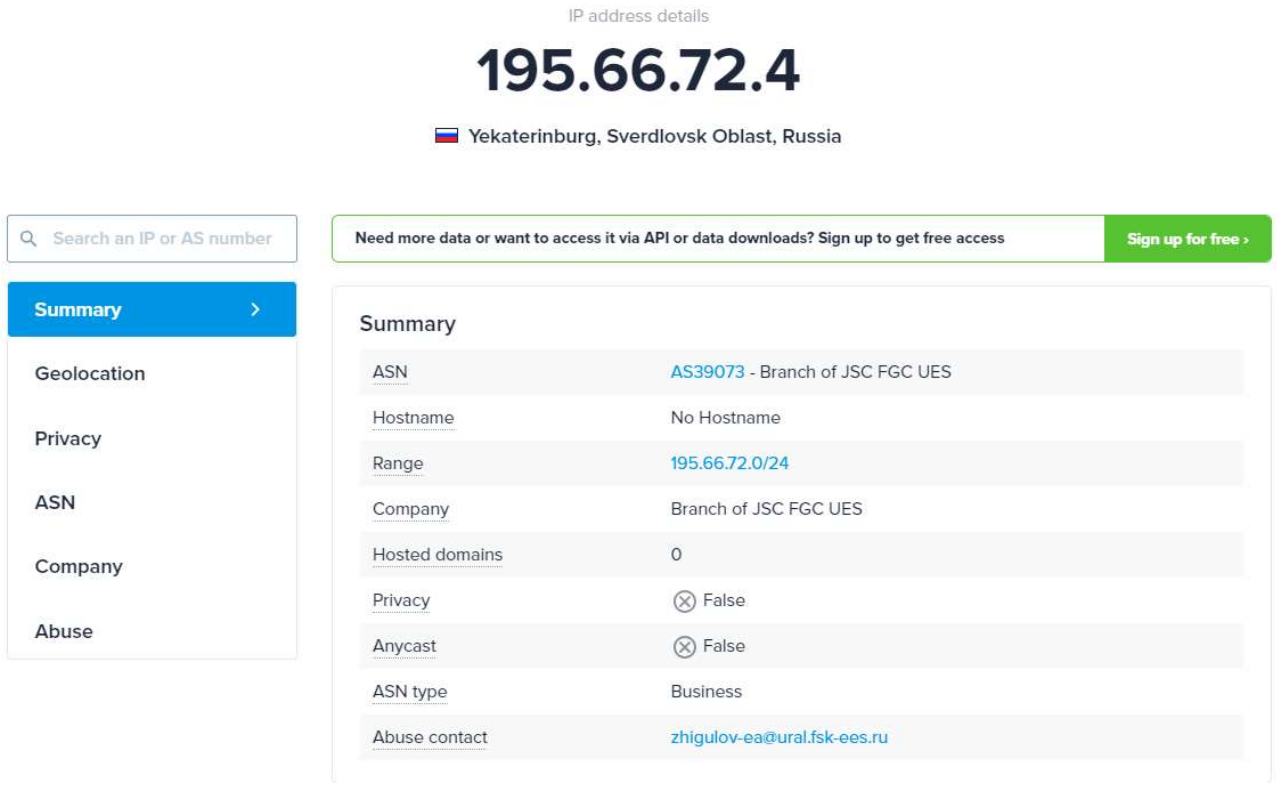
The discovery of the Pipedream malware toolkit represents a rare addition to the handful of malware specimens found in the wild that target industrial control systems (ICS) software. The first and still most notorious example of that sort of malware remains Stuxnet, the US- and Israeli-created code that was uncovered in 2010 after it was used to destroy nuclear enrichment centrifuges in Iran. More recently, the Russian hackers known as Sandworm, part of the Kremlin's GRU military intelligence agency, deployed a tool called Industroyer or Crash Override to trigger a blackout in the Ukrainian capital of Kyiv in late 2016.

The next year, Kremlin-linked hackers infected systems at the Saudi Arabian oil refinery Petro Rabigh with a piece of malware known as Triton or Trisis, which was designed to target its safety systems—with potentially catastrophic physical consequences—but instead triggered two shutdowns of the plant's operations. Then, just last week, Russia's Sandworm hackers were detected using a new variant of their of Industroyer code to target a regional electrical utility in Ukraine, though Ukrainian officials say they managed to detect the attack and avert a blackout.

The Pipedream advisory serves as a particularly troubling new entry in the rogue's gallery of ICS malware, however, given the breadth of its functionality. But its revelation—apparently before it could be used for disruptive effects—comes in the midst of a larger crackdown by the Biden administration on potential hacking threats to critical infrastructure systems, particularly from Russia. Last month, for instance, the Justice Department unsealed indictments against two Russian hacker groups with a history of targeting power grids and petrochemical systems. One indictment named for the first time one of the

hackers allegedly responsible for the Triton malware attack in Saudi Arabia and also accused him and his co-conspirators of targeting US refineries. A second indictment named three agents of Russia's FSB intelligence agency as members of a notorious hacker group known as Berserk Bear, responsible for years of electric utility hacking. And then early this month the FBI took measures to disrupt a botnet of networking devices controlled by Sandworm, still the only hackers in history known to have triggered blackouts.

Even as the government has taken measures to call out and even disarm those disruptive hackers, Pipedream represents a powerful malware toolkit in unknown hands—and one from which infrastructure operators need to take measures to protect themselves, says Caltagirone. “This is not a small deal,” he says. “It’s a clear and present danger to the safety of industrial control systems.” (both ours and theirs).



195.66.72.0/24

Network Info | Whois | DNS | IRR | Propagation | Visibility | Routes | Traceroute

Visibility 100% (655 out of 655) Full Views

Collector	Peer IP	Peer ASN	Has Prefix	Origin ASN
collector14.bgp.he.net	172.18.14.1	6939	x	39073
collector14.bgp.he.net	172.18.14.2	6939	x	39073
route-views2.saopaulo	187.16.216.232	28329	x	39073
route-views2.saopaulo	187.16.209.34	271253	x	39073
route-views2.saopaulo	187.16.219.247	263541	x	39073
route-views2.saopaulo	187.16.222.16	199524	x	39073
route-views2.saopaulo	187.16.222.221	263009	x	39073
route-views2.saopaulo	187.16.219.29	16552	x	39073
route-views2.saopaulo	187.16.218.138	268976	x	39073
route-views2.saopaulo	187.16.220.229	49544	x	39073
route-views2.saopaulo	187.16.214.101	53427	x	39073
route-views2.saopaulo	187.16.219.20	61832	x	39073
route-views2.saopaulo	187.16.215.63	264409	x	39073
route-views2.saopaulo	187.16.222.156	264479	x	39073
route-views2.saopaulo	187.16.222.229	199524	x	39073
route-views2.saopaulo	187.16.222.168	262791	x	39073
route-views2.saopaulo	187.16.221.193	37468	x	39073
route-views2.saopaulo	187.16.209.243	271253	x	39073
route-views2.saopaulo	187.16.217.27	28329	x	39073
route-views2.saopaulo	187.16.220.216	52873	x	39073
route-views.napafrica	196.60.8.113	328512	x	39073
route-views.napafrica	196.60.10.62	16552	x	39073
route-views.napafrica	196.60.8.152	3491	x	39073
route-views.napafrica	196.60.8.60	37468	x	39073
route-views.napafrica	196.60.10.195	328964	x	39073
route-views.napafrica	196.60.8.6	49544	x	39073
route-views.napafrica	196.60.8.142	37271	x	39073
route-views.napafrica	196.60.9.139	32653	x	39073