

Anonymous vendetta targets Russia

Russia, no stranger to cyberwarfare, has come under a barrage of cyberattacks from *Anonymous* "hacktivists" since its invasion of Ukraine

WHO ARE "ANONYMOUS"?

Decentralised collective of international hackers who exploit weaknesses in computer systems to promote their political agenda – generally attacking organisations accused of misusing power

NOTEWORTHY CYBERATTACKS



Feb 24: Anonymous Twitter account @YourAnonOne, tweets: *The Anonymous collective is officially in cyber war against the Russian government*

Russian Center for the Protection of Monuments website defaced with pro-Ukraine artwork. Circus melody *Entrance of the Gladiators* plays for 10 hours



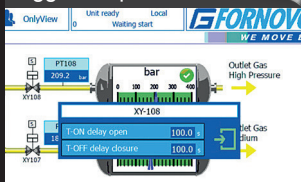
RT State TV station temporarily taken off air

Feb 25: Russian **Ministry of Defence** website disabled, data leaked online

Feb 26: Russian military radio communications leaked

Numerous state TV channels hacked to show videos of war in Ukraine (*hack repeated on Mar 6 to include streaming services*)

Feb 27: **Linux** terminal hacked. Breach of gas control system in North Ossetia almost triggers explosion



Roscosmos space agency website hacked and defaced



Maritime tracking data hacked to change call sign of \$100m yacht *Graceful* – allegedly owned by Putin – to *FCKPTN* and set target destination to *Hell*

Feb 28: **Cyber Partisans*** hack Belarus rail network, slowing transportation of Russian troops to Ukraine

Mar 1: **Ministry of Economic Development** database leaked

Mar 3: Anonymous says it has hacked over 2,500 Russian and Belarusian government sites, including state media outlets, banks, hospitals and airports

Hacktivists often wear **Guy Fawkes** masks, as portrayed in graphic novel *V for Vendetta*



Mar 12: Russian military radios, using frequency 4625kHz, jammed

Mar 13: **Rosatom**, state-owned atomic energy company hacked, with gigabytes of data leaked

Mar 14: 20TB of data at **Rosneft**, Russia's leading oil company, vandalised

Overview	Indices	Browser	Structured Query	Any Request
putin_stop_this_war	3qvt	2838/2838	0	
putin_stop_this_war	4pfz	2838/2838	0	
putin_stop_this_war	5u4od	2838/2838	0	
putin_stop_this_war	5nfesb	2838/2838	0	
putin_stop_this_war	64eu	2838/2838	0	
putin_stop_this_war	6qjft	2838/2838	0	
putin_stop_this_war	7zewh	2838/2838	0	
putin_stop_this_war	8pida	2838/2838	0	
putin_stop_this_war	ajyc	2838/2838	0	
putin_stop_this_war	bapj	2838/2838	0	
putin_stop_this_war	bkmdb	2838/2838	0	
putin_stop_this_war	bvtzmn	2838/2838	0	
putin_stop_this_war	c432y	2838/2838	0	
putin_stop_this_war	cfmda	2838/2838	0	

Mar 16: Analysis of Russian databases finds 92 out of 100 compromised, with file names changed to *Putin stop this war*, *Glory to Ukraine*, and other pro-Ukrainian slogans

Website of **Ministry of Emergencies** hacked to display hyperlink that reads *Don't trust the Russian media – they are lying*

Squad303's online tool **1920.in** allows public to text Russian cell phones – claims 30m SMS messages sent to date

Mar 17: Anonymous claims to have tripled strength of attacks against Russia since invasion began

Attacks continue...

Mar 6: Russian military shortwave radios hacked to display infamous **Trollface†** image on equipment screens

Mar 9: More than 400 Russian CCTV cameras hacked to display anti-Putin messages. Some live feeds compiled into website *behindenemylines.live*

Mar 10: **Roskomnadzor** (agency that controls Russian mass media) sees 360,000 files leaked onto internet

Mar 11: New Polish Anonymous affiliate, **squad303**, sends 7 million SMS messages to Russian cell phones – *The Kremlin is lying. Find out the truth about Ukraine on the free internet and in the Telegram app. Time to overthrow dictator Putin!*

