Ukraine

Anonymous: the hacker collective that has declared cyberwar on Russia

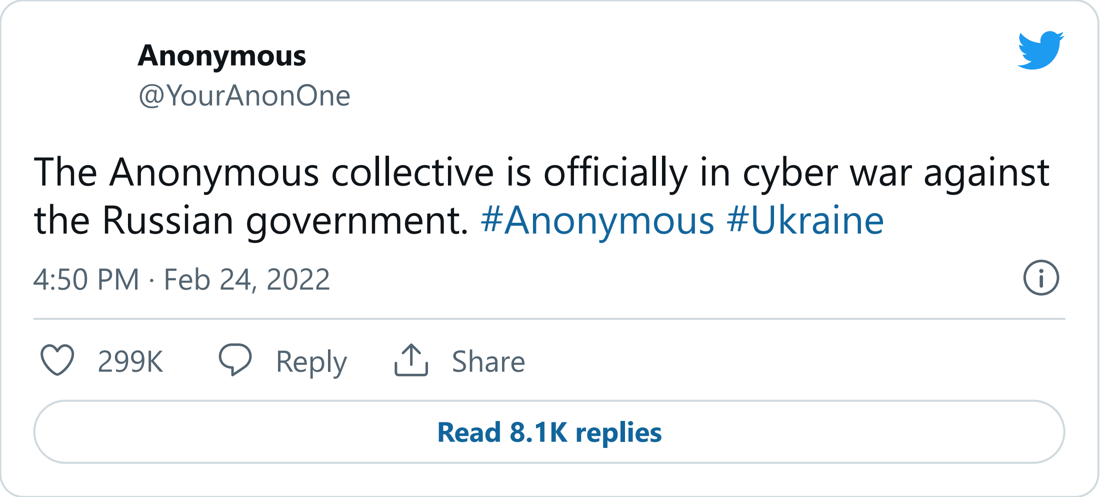
The group has claimed credit for hacking the Russian Ministry of Defence database, and is believed to have hacked multiple state TV channels to show pro-Ukraine content

- Russia-Ukraine war latest news: follow live updates

Dan Milmo *Global technology editor*

Sun 27 Feb 2022 13.51 EST

Cyber conflicts are fought in the shadows, but in the case of Russia's invasion of Ukraine, it is a group that calls itself Anonymous that has made the most public declaration of war. Late on Thursday the hacker collective tweeted from an account linked to Anonymous, @YourAnonOne, that it had Vladimir Putin's regime in its sights.



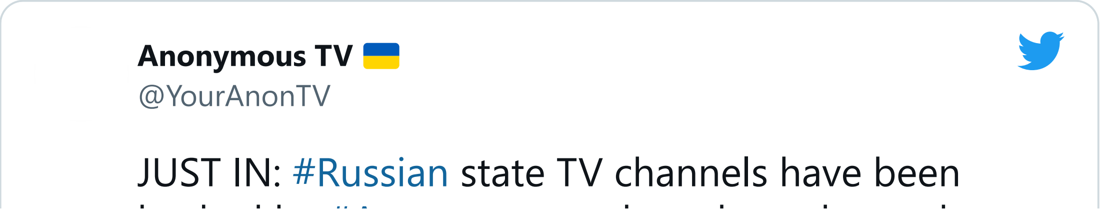
Anonymous
@YourAnonOne

The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine

4:50 PM · Feb 24, 2022

In the days since, the group has claimed credit for several cyber incidents including distributed denial of service attacks - where a site is rendered unreachable by being bombarded with traffic - that have brought down government websites and that of Russia Today, the state-backed news service. The DDoS attacks still appeared to be working on Sunday afternoon, with the official sites for the Kremlin and Ministry of Defence still inaccessible.

Anonymous also said it had hacked the Ministry of Defence database, while on Sunday it was claimed the group had hacked Russian state TV channels, posting pro-Ukraine content including patriotic songs and images from the invasion.



Anonymous TV 🇺🇦
@YourAnonTV

JUST IN: #Russian state TV channels have been hacked by #Anonymous to broadcast the truth about what happens in #Ukraine.

#OpRussia #OpKremlin #FckPutin #StandWithUkriane

Watch on Twitter

4:03 PM · Feb 26, 2022

Read the full conversation on Twitter

222.7K Reply Share

Read 4.5K replies

BECZKA ✌
@beczka_tv

Someone hacked into Russian state TV channels. They feature Ukrainian music and national symbols. 🇺🇦

Internet users suspect that this may be another action by the hacker group #Anonymous, which declared a cyber war to Russia in connection with the attack on #Ukraine.

Watch on Twitter

8:57 AM · Feb 26, 2022

8.4K Reply Share

Read 156 replies

The group's nature as an informal collective makes it difficult to attribute these attacks to Anonymous definitively. Jamie Collier, a consultant at US cybersecurity firm Mandiant, said: "It can be difficult to directly tie this activity to

Anonymous, as targeted entities will likely be reluctant to publish related technical data. However, the Anonymous collective has a track record of conducting this sort of activity and it is very much in line with their capabilities."

Its targets in the past have included the CIA, the Church of Scientology and Islamic State, and although the collective was left reeling by a number of arrests in the US in the early 2010s, it revived activity after the murder of George Floyd. One former Anonymous member has described its guiding principle as "anti-oppression".

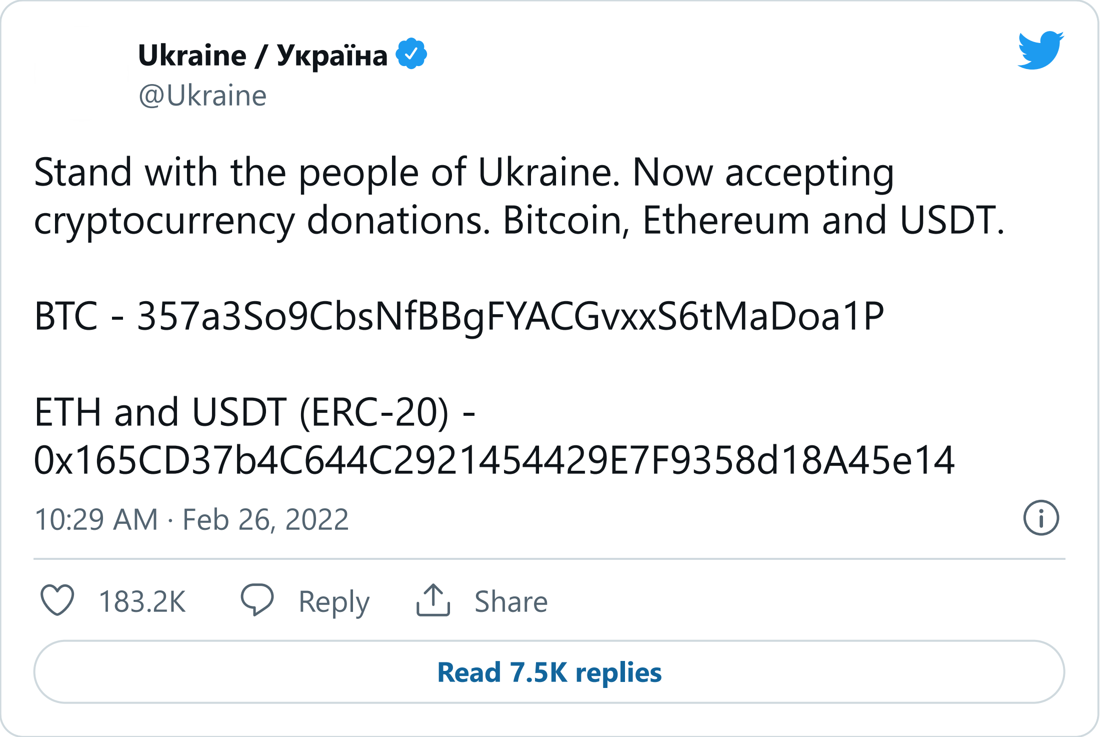
Russia Today openly attributed the problems with its website to Anonymous, and claimed the attacks came from the US after the group had published its "declaration of war". A spokesperson for the channel said: "After the statement by Anonymous, RT's websites became the subject of massive DDoS attacks from some 100 million devices, mostly based in the US."

By contrast, cyber activity against Ukraine has been muted so far, despite widespread predictions that a Russian military assault on the country would be combined with digital shock and awe. Ukrainian websites were hit with DDoS attacks ahead of the offensive, including the Ukrainian defence ministry and PrivatBank, Ukraine's largest commercial bank, but there has been nothing on the scale of the NotPetya assault in 2017 - when a devastating malware attack attributed to Russia destroyed computers in Ukraine and around the world. Cloudflare, a US tech firm that protects companies against DDoS attacks, described the initial denial of service sorties last week as "relatively modest". The UK and US governments have already blamed an earlier set of DDoS attacks against Ukrainian websites, on 15 and 16 February, on Moscow.

As with the attacks claimed by Anonymous, DDoS salvos are designed to sow confusion and damage morale, whereas malware can cause serious and irreparable damage. NotPetya, a so-called wiper virus that was inserted into tax accounting software used by Ukrainian firms but spilled into other countries, caused $10bn (£7.5bn) of damage worldwide by encrypting computers permanently.

Last week Ukraine was hit by an attempted wiper attack, via a new strain of malware dubbed HermeticWiper that prevented computers from rebooting. However, the scale of the attack left only several hundred machines affected and its geographic reach beyond Ukraine has been limited to Latvia and Lithuania.

There have been cyber skirmishes elsewhere in the conflict. Partial restrictions have been imposed on Facebook by the Russian government after officials accused the social network of censoring state-backed media on the platform, prompting Facebook to ban ads from Russian state media. Google's YouTube platform has also banned state media adverts. Another US tech titan, Elon Musk, is providing satellite internet access to Ukraine via his Starlink satellites, while the Ukrainian government is openly seeking international donations in cryptocurrency and has reportedly received millions of dollars in response.



Ukraine / Україна ✓
@Ukraine

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - 357a3So9CbsNfBBgFYACGvxxS6tMaDoa1P

ETH and USDT (ERC-20) -
0x165CD37b4C644C2921454429E7F9358d18A45e14

10:29 AM · Feb 26, 2022

Nonetheless, the cyber dimension to the Ukraine conflict has been low-key up to this point. Ciaran Martin, professor of practice at the Blavatnik school of government at Oxford University and former head of the UK's National Cyber Security Centre, says cyber has played "remarkably little part" in the conflict, at least so far.

"The cyber activity from Russia against Ukraine has been there, but is consistent with Russia's cyber harassment of the country going back years. Similarly, from what we can see, the response against Russia from the west has not had a strong cyber component so far - it has been about stringent sanctions. All of this might change, and the west is right to remain on high alert for increased cyber activity."

The truth, they say, is the first casualty of war, more so at a time when misinformation spreads so rapidly. But with correspondents on the ground on both sides of the Ukraine-Russia border, in Kyiv, Moscow, Brussels and other European capitals, the Guardian is well placed to provide the honest, factual reporting that readers will need to understand this perilous moment for Europe and the former Soviet Union.

The Guardian has an illustrious history of persistent, independent reporting in the region. We know there is no substitute for being there, and were on the ground at all the critical moments - from the 1917 revolution and the Ukrainian famine of the 1930s, to the collapse of 1991 and the first Russo-Ukrainian conflict in 2014. And we will stay on the ground through this frightening period as well.

Tens of millions have placed their trust in the Guardian's fearless journalism since we started publishing 200 years ago, turning to us in moments of crisis, uncertainty, solidarity and hope. We'd like to invite you to join more than 1.5 million supporters, from 180 countries, who now power us financially - keeping us open to all, and fiercely independent.

Unlike many others, the Guardian has no shareholders and no billionaire owner. Just the determination and passion to deliver high-impact global reporting, always free from commercial or political influence. Reporting like this is vital for democracy, for fairness and to demand better from the powerful.

And we provide all this for free, for everyone to read. We do this because we believe in information equality. Greater numbers of people can keep track of the global events shaping our world, understand their impact on people and communities, and become inspired to take meaningful action. Millions can benefit from open access to quality, truthful news, regardless of their ability to pay for it.

If there were ever a time to join us, it is now. Every contribution, however big or small, powers our journalism and sustains our future. **Support the Guardian from as little as $1 - it only takes a minute. Thank you.**

Single [✓ Monthly] Annual

$7 per month [✓ $15 per month] Other

Continue →

Remind me in April

VISA mastercard AMERICAN EXPRESS PayPal