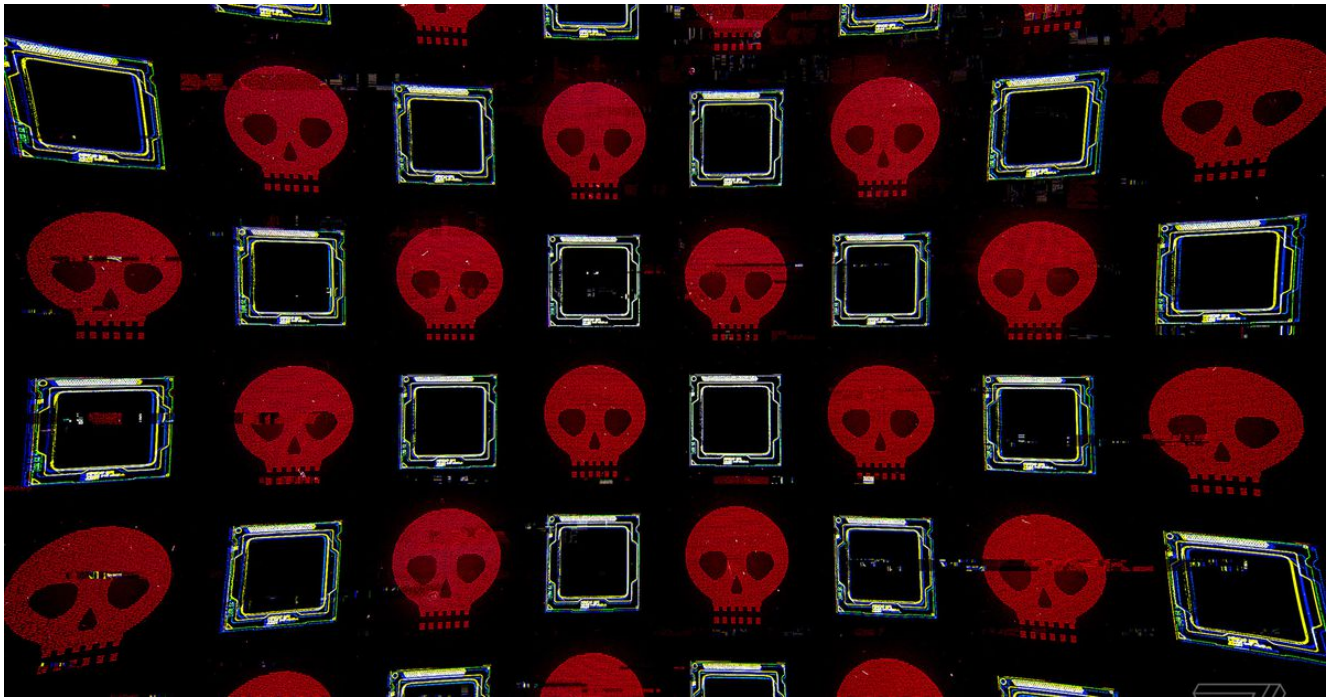


Ukrainian defense ministry hit by DDoS during tense standoff with Russia



On Tuesday, Ukraine's Ministry of Defence suffered from a DDoS attack that prevented users from accessing its website, and two Ukrainian banks lost access to online banking services, according to statements from the government.

In a tweet posted at around 7PM local time (12PM ET), the Ukrainian Ministry of Defence said that its website was probably being hit with a DDoS attack and that work to restore service was underway. Four hours later, the site still could not be accessed.

PrivatBank faced a "massive DDoS attack" that blocked online banking services, including payments and balance inquiries. The DDoS attack comes as Russia has claimed to be de-escalating potential conflict by withdrawing troops from the Ukraine border – a statement that was met with "cautious optimism" by NATO but has also faced skepticism amid a series of contradictory signals from the Russian military.

At the same time, two banks also suffered from a denial-of-service attack that took ATMs offline and prevented some clients from withdrawing or transferring funds online.

According to a statement from the Ukrainian government's Center for Strategic Communications, PrivatBank faced a "massive DDoS attack" that blocked many online banking services, including payments and balance inquiries, but did not affect core banking services or threaten customer funds. Oschadbank also lost all online banking functionality, according to the statement. A few hours later, another statement from the Ukrainian government said that the banks had resumed online service.

The cyberattack has still not been attributed to a specific actor by the Ukrainian government or US officials, although in light of the ongoing military situation, many suspect Russian involvement.

Opinions are divided on whether today's attacks – which are relatively commonplace in terms of Russia-Ukraine relations – represent a precursor to military activity or a return to normalcy. Matt Tait, a security analyst known by the moniker pwnallthethings, tweeted that the DDoS was not "part of the invasion" and urged caution in reporting.

Other sources in the cybersecurity industry similarly downplayed the severity of the attack. "We can confirm the DDOS attacks but do not see any indication that their impact is critical...this activity could be to keep a sense of pressure on Ukraine in the face of more positive news over the past day," said Cisco's director of threat intelligence Matthew Olney, per a tweet shared by cybersecurity journalist Kim Zetter.

But according to reports in *The Washington Post*, recently declassified intelligence suggests that Russian government hackers are likely to have already compromised critical

Ukrainian infrastructure and would unleash much more damaging attacks in the event of an invasion.

The *Post*'s report cites an official familiar with the intelligence documents to claim that Russia would be able to disrupt services like electricity, transport, finance, and telecommunications, either in direct support of military operations or to create a sense of panic that would destabilize the country.

Reached by email, a representative of the Cybersecurity and Infrastructure Security Agency (CISA) declined to provide a statement on the situation but directed *The Verge* to an information page detailing preparedness measures being taken to reduce the likelihood of a Russian cyberattack against the US.

<https://www.theverge.com/2022/2/15/22936192/ukraine-defense-ministry-ddos-russia-conflict-de-escalation>