The websites of Ukraine's defense, foreign and interior ministries were unreachable or painfully slow to load Thursday morning after a punishing wave of distributed-denial-of-service attacks as Russia struck at its neighbor, explosions shaking the capital of Kyiv and other major cities.

In addition to DDoS attacks on Wednesday, cybersecurity researchers said unidentified attackers had infected hundreds of computers with destructive malware, some in neighboring Latvia and Lithuania.

Asked if the denial-of-service attacks were continuing Thursday morning, senior Ukrainian cyber defense official Victor Zhora did not answer. "Are you serious?" he texted. "There are ballistic missiles here."

"This is terrible. We need the world to stop it. Immediately," Zhora said of the offensive that Russian President Vladimir Putin announced in the pre-dawn hours.

Officials have long expected cyber attacks to precede and accompany any Russian military incursion. The combination of DDoS attacks, which bombard websites with junk traffic to render them unreachable, and malware infections hewed to Russia's playbook of wedding cyber operations with real-world aggression.

ESET Research Labs said it detected a previously unseen piece of data-wiping malware Wednesday on "hundreds of machines in the country." It was not clear how many networks were affected.

"With regards whether the malware was successful in its wiping capability, we assume that this indeed was the case and affected machines were wiped," said ESET research chief Jean-Ian Boutin. He would not name the targets but said they were "large organizations."

Image source: First Post

ESET was unable to say who was responsible.

Symantec Threat Intelligence detected three organizations hit by the wiper malware — Ukrainian government contractors in Latvia and Lithuania and a financial institution in Ukraine, said Vikram Thakur, its technical director. Both countries are NATO members.

“The attackers have gone after these targets without much caring for where they may be physically located,” he said.

All three had “close affiliation with the government of Ukraine,” said Thakur, saying Symantec believed the attacks were “highly targeted.” He said roughly 50 computers at the financial outfit were impacted, some with data wiped.

Asked about the wiper attack on Wednesday, Zhora had no comment.

Boutin said the malware’s timestamp indicated it was created in late December.

“Russia likely has been planning this for months, so it is hard to say how many organizations or agencies have been backdoored in preparation for these attacks,” said Chester Wisniewski, principal research scientist at the cybersecurity firm Sophos. He guessed the Kremlin intended with the malware to “send the message that they have compromised a significant amount of Ukrainian infrastructure and these are just little morsels to show how ubiquitous their penetration is.”

Word of the wiper follows a mid-January attack that Ukrainian officials blamed on Russia in which the defacement of some 70 government websites was used to mask intrusions into government networks in which at least two servers were damaged with wiper malware masquerading as ransomware.

Cyberattacks have been a key tool of Russian aggression in Ukraine since before 2014, when the Kremlin annexed Crimea and hackers tried to thwart elections. They were also used against Estonia in 2007 and Georgia in 2008. Their intent can be to sow panic, confuse and distract.

Distributed-denial-of-service attacks are among the least impactful because they don’t entail network intrusion. Such attacks barrage websites with junk traffic so they become unreachable.

The DDoS targets Wednesday included the defense and foreign ministries, the Council of Ministers and Privatbank, the country’s largest commercial bank. Many of the same sites were similarly knocked offline Feb. 13-14 in DDoS attacks that the U.S. and U.K. governments quickly blamed on Russia’s GRU military intelligence agency

Wednesday’s DDoS attacks appeared less impactful than the earlier onslaught — with targeted sites soon reachable again — as emergency responders blunted them. Zhora’s office, Ukraine’s information protection agency, said responders switched to a different DDoS protection service provider.

Doug Madory, director of internet analysis at the network management firm Kentik Inc., recorded two attack waves each lasting more than an hour.

A spokesman for California-based Cloudflare, which provides services to some of the targeted sites, said Wednesday that DDoS attacks in Ukraine had been until then sporadic but on the rise in the past month but “relatively modest compared to large DDoS attacks we’ve handled in the past.”

The West blames Russia’s GRU for some of the most damaging cyberattacks on record, including a pair in 2015 and 2016 that briefly knocked out parts of Ukraine’s power grid and the NotPetya “wiper” virus of 2017, which caused more than $10 billion of damage globally by infecting companies that do business in Ukraine with malware seeded through a tax preparation software update.

The wiper malware detected in Ukraine this year has so far been manually activated, as opposed to a worm like NotPetya, which can spread out of control across borders.

Subscribe to the International Relations Updates by The Kootneeti

* indicates required

Full Name

Email Address *

Subscribe

made with mailchimp

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments