FROM HTTPS://OGLOBO.GLOBO.COM/MUNDO/UCRANIA-CONVOCOU-EXERCITO-DE-TI-CONTRA-ACOES-CIBERNETICAS-RUSSAS-MAS-MOSCOU-AINDA-NAO-USOU-SEU-POTENCIAL-NA-GUERRA-ATUAL-25428642

≡ O GLOBO WORLD

WORLDWAR IN UKRAINE

Ukraine Summoned 'IT Army' Against Russian Cyber Actions, But Moscow Has Not Used Its Potential in Current War

Ukrainian defense resources have been bolstered and subject to attacks since 2014, and officials promise to react to possible Moscow attacks on their systems.

Filipe Barini

03/13/2022 - 05:30 / Updated on 03/13/2022 - 15:50

Computer screen infected with the virus that "hijacks" files, such as NotPetya, in 2017 Photo: Simon Dawson / Bloomberg

newsletters

Hours before Russian troops began their invasion of Ukraine, dozens of websites of Ukrainian institutions and banks were inaccessible in what local authorities and digital monitoring services said was an attack on the country — the third of its kind this year .

“Another DDoS attack against our state has begun,” Ukrainian Minister of Digital Transformation Mykhailo Fedorov said on Telegram on February 24, using the acronym for “distributed denial of service attack”, when a coordinated action, with multiple machines, brings down a certain system. That same day, digital security companies, such as Symantec, pointed out that computers in Ukraine were also the target of “malicious software” (malware) responsible for erasing data from infected machines.

Understand: For analyst, wrong calculation can explain Russian cyber silence

Alongside the signs of a conventional invasion, there were fears in Kiev that the military strike would be accompanied by actions against Ukraine's strategic systems , including power transmission networks. After all, since 2014, when Euromaidan ousted pro-Moscow President Viktor Yanukovych and an anti-Russian government came to power, massive cyberattacks are routine.

Before the conflict: After failure of negotiations between Russia and NATO, Ukraine suffers hacker attack and government websites go down

As part of the defense plans, now focusing on the current conflict and the possibility of using a “digital arsenal”, the government of Ukraine, which had already been summoning volunteers from all over the world to the front, also made an appeal to hackers and security experts. “We are creating an IT (Information Technology) army. We need digital talent,” wrote Minister Fedorov on Twitter on February 26. “There will be tasks for everyone. We will continue to fight on the cyber front.”

Today, there are about 35,000 subscribers to the Telegram channel used for the call, but it is not known exactly how many are “soldiers” or how many are journalists, researchers or just curious. Most of the tasks are defensive, but there is the possibility that they can be used in offensive actions against Russia.

“The point here is that we're under attack, and we never react. We just defend ourselves. So for the first time, let's try to show them [Russians] what it feels like to have their infrastructure attacked, when it's like not being able to use bank cards or government services." .

New 'battleground': Hackers take center stage in great-power strategy

Despite great expectations, experts heard by GLOBO are a little more skeptical about the “digital troop”.

"The impacts of this group cannot yet be verified, but it is likely that, within an armed conflict, their operations will be negligible at best," said Lukasz Olejnik, an independent cybersecurity researcher and former Red Cross consultant in Geneva. .

Stuart Madnick, professor of Information Technology at the Sloan School of Management at the Massachusetts Institute of Technology, in turn, points out that it is not always necessary to have so many resources, both technical and human, for an operation of this type.

“I don't know how effective they are, but you don't need a lot of people to wreak havoc. I haven't spoken to them and I don't know what they have in their hands. But I believe there is a public relations aspect to having so many outsiders coming to help you,” he told GLOBO.

Alert: US, EU and NATO accuse China of hacking Microsoft server in global cyberattack campaign

It has not yet been possible to verify on a large scale the capabilities of the Ukrainian “IT Army”: contrary to what was expected, Russia has avoided repeating past actions against Ukraine. In 2015 and 2016, attacks toppled power transmission systems, leaving thousands of people without power, including in Kiev.

— In this conflict, we did not have high impact cyberattacks. They are not being enforced, perhaps with the exception of the effects of some data-destroying malware causing problems in border control systems,” points out Lukasz Olejnik. “How the cyber element is used will depend on how the conflict plays out in the future. Impact cyberattacks cannot be fended off, but they are not a certainty. It all depends on the goals of their authors.

Defenses

In recent years, Ukraine has been receiving foreign aid to develop its defense from independent consultants and the US government, with multimillion-dollar investments. The objective: to prepare the country for the worst possible scenario.

An example of this strategy was reported by the Financial Times earlier this month: months before the war began, US consultants traveled to Ukraine for a “scan” for malicious programs that could wipe out data and entire systems.

'Parallel' financial system: Cryptocurrencies help fund Ukraine's government support groups, report claims

According to the newspaper, one of the malware was found in the state-owned train company, precisely one of the main means used by Ukrainians to flee the country. If it had been triggered, thousands of people could be prevented from continuing their journey.

"For sure there are so many, so many undiscovered actions that have left some malware capable of being activated," VS Subrahmanian, a professor of computer science at Northwestern College, told the Financial Times. “It's like a bomb planted in your own house: it's harmless until it's activated.

It is not clear why Russia, which theoretically has the capacity to launch large actions, has not yet made massive use of the cyber weapon.

Some analysts point to an answer: Russian forces played down Ukrainian capabilities, and felt that the “shock and awe” strategy would not require unconventional tools. An argument in favor of this thesis comes from the battlefields themselves, with the military setting aside secure communication systems and using ordinary cell phones or civilian radios, which are easily intercepted and blocked.

Smeared image?: Russia exposes Ukraine's military flaws that could be exploited by adversaries in the future

Another hypothesis has to do with war planning, not only immediate, but in the medium and long term: Stuart Madnick, from MIT, recalls that large-scale attacks can easily spread to other countries, even if they target a specific system. .

He cites the case of Stuxnet , a virus used by the US and Israel that in 2010 wreaked havoc at the Natanz nuclear plant in Iran, but also affected computers in Indonesia, Azerbaijan and the US itself. Another example is the NotPetya virus in 2017, which "hijacked" computers and systems and demanded payment for its release. The action was considered the largest in US history and attributed to Russia.

— NotPetya targeted Ukrainian businesses, but some of those businesses were subsidiaries of multinational companies. And as soon as the virus entered these computers, it quickly spread through the networks of global companies, and all of them had their activities suspended for long periods - said the expert.

Still talking about possible worst-case scenarios, Mednick recalled that, unlike combat in the non-virtual world, it is not always easy to find out where the cyberattack came from, which could lead to wrong conclusions or actions aimed at blaming the enemy side.

"When someone fires a cannon, you have a pretty good idea where it was fired. When it comes to a cyberattack, it is very difficult to determine this. An acquaintance of mine who works with this always tells me that a very good hacker is one who knows how to leave evidence that points to anyone else," Madnick concluded.