The increasing presence of pro-Russia hacktivists

channellife.com.au/story/the-increasing-presence-of-pro-russia-hacktivists

Tom Raynel

By Tom Raynel, Managing Editor

A new advisory report released by Radware, a global leader of cyber security and application delivery solutions for physical, cloud, and software-defined data centres, has highlighted a pro-Russian hacktivist group called Zarya.

The group, which operated initially as a special force's unit under Killnet, is building Mirai variants to increase the attack power of the DDoS botnet it uses to perform attacks on the West.

Zarya's propaganda website, known as 'Zarya - CyberFront,' and its attack campaign log and malware is hosted by Akur Group, a hosting provider for pro-Russian hacktivist groups.

With the Russian/Ukrainian conflict now in its second year, this recent activity is significant because it demonstrates how pro-Russian hacktivists have evolved their tools, techniques, and procedures over time.

Pro-Russian hacktivists have moved beyond the basic denial-of-service scripts and crowdsourced attacks to more advanced and potent techniques. This even means leveraging and cooperating with other hacktivist groups within the Russian-speaking community to achieve their goals.

The digital threat actors involved have become more organized and sophisticated. In addition, social communities have emerged supporting these malicious activities through social media and online groups on various platforms.

This growing influence has resulted in a proliferation of malicious activities and the spread of sophisticated tools and techniques across the internet. Not only this, but even the support of criminal activities such as buying and selling stolen data or hosting malware used in cyber-attacks.

Zarya - who are they?

Zarya, which translates to "dawn," is a pro-Russian hacktivist group that emerged in March 2022. Initially, the group operated as a special forces unit under the command of Killnet.

Zarya's objectives have evolved as the conflict between Russia and Ukraine has progressed. This led to a breakaway from Killnet, with the group at times going by 0x000000.

It led to a focus on recruiting skilled hackers from other pro-Russian threat groups that were burning out in the spring of 2022.

In May 2022, Zarya rejoined Killnet as part of a larger project, translated as, 'Legion.' During the summer of 2022, the group, Zarya Legion, established itself as a leading force, setting an example for other groups and eventually becoming an independent entity known as just Zarya in August 2022.

As for what Zarya does, the group is primarily known for its involvement in Denial-of-Service attacks, website defacement campaigns, and data leaks.
These operations have been leveraged to support the group's pro-Russian agenda and have significantly disrupted targeted organizations and individuals who wish to threaten Russia's position geopolitically.

Zarya's CyberFront website provides information about targets for the pro-Russian hacktivist group. According to the website, the group primarily targets government agencies, service providers, critical infrastructure, and civil service employees almost entirely internationally.

The website currently features links to 48 different hacking campaigns carried out by the group, along with the corresponding leaked data. Allegedly, 655 Gigabytes worth of data has been leaked, which is a very serious revelation considering the security implications of such a large leak.