MAZEBOLT

September 2022

DDoS Attack Round Up

The Major DDoS Attack Trends of September

As we finish Q3, politically motivated malicious threat actors continue to target governmental organizations. This monthly trend follows the significant increase in patriotic DDoS attacks related to the Russo-Ukrainian conflict in H1 and a general rise in DDoS attacks. Pro-Russian and pro-Iranian hacktivists specifically have become more active as the political landscape has changed dramatically.

Global governments at risk as patriotic DDoS attacks spread

Russia and Ukraine

Russia's electronic document management system was attacked at the beginning of the month, hitting multiple banks, supermarkets, and schools. The Ministry of Industry and Trade believes pro-Ukrainian hackers to be responsible for the attacks.

Ukraine's Monobank went down this month for the second time this year. The earlier attack in February also included multiple Ukrainian banks such as Alfa-Bank, Raiffeisen Bank, PrivatBank and Oschadbank.

Experts claim that DDoS attacks on electric supplies will increase as Russia strengthens his efforts in Ukraine, after a stunning counter-offensive by Ukrainian forces.

Nordic region and Europe

In the Nordic region, the website of the Swedish Election Authority was hit by three DDoS attacks during the general election for two days. As the vote in the election was counted, the Bonnier News group in Sweden and other news groups sharing the same infrastructure were inaccessible for about an hour.

These attacks on the Nordic region follow the trend of continued attacks on the area as it prepares to join NATO.

DDoS attacks unrelated to the Russo-Ukrainian war also continue, however. The Balkan Investigative Reporting Network (BIRN) news outlet reported DDoS attacks earlier this month. The motive was most likely an attempt to take down a page about Yasam Ayavefe, a Turkish businessman who was found guilty of buying honorary Greek citizenship.

Asia

A barrage of DDoS attacks has also hit Japan. Its electronic government website suffered downtime intermittently for several days in addition to 20 other government websites such as the Digital Agency, the Internal Affairs and Communications Ministry, the Education, Culture, Sports, the Technology Ministry, and the Imperial Household Agency. The website of one of its largest ports, Nagoya Port Authority, was also down for almost an hour on September 6th.

This attack is believed to be executed by Killnet, a pro-Russian hacktivist group that has targeted government agencies around the world and strengthened its activity since the invasion of Ukraine.

Other hacktivist groups have gained traction in India. Mysterious Team Bangladesh (MT) is a new group that has targeted both domains and sub-domains of multiple Indian governmental websites. MT has been linked to an Indonesian-based hacktivist group.

Iran

Hacktivist group Anonymous claimed responsibility for taking down the website of the Iranian Central Bank this month. The group claimed to attack in solidarity with the protests of the death of Mahsa Amini. Her death at the hands of Iranian authorities sparked worldwide protests and outcries from various human rights organizations.

Gaming Still Continues to Be Target for DDoS

Not all attackers are political, so the gaming industries will always be targets for DDoS attacks.

Blizzard Entertainment was hit again this month after DDoS attacks in May and repeated attacks last year. Flutter Entertainment also suffered one of the worst outages in history, with 18 hours of disruption.

But DDoS threats extend beyond gaming as well. As the operator of Flutter Entertainment aptly reported in an official statement: “Such events are a constant threat to every company operating online, and we are no different.”

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Sep-01	Russia	Government	2 days	-	The Ministry of Industry and Trade	The attack could have been avoided with proper protection	Link
Sep-02	Bosnia	Media	3 days	2 days	Balkan Investigative Reporting Network & Solomon, a Greek independent media outlet	35M IP connections from all over the world. The attack was aimed at a page about a Turkish convicted of fraud bought his way to honorary Greek citizenship	Link
Sep-06	Japan	Government	2 days	-	20 Government Websites including the tax authority	e-Gov website inaccessible by cyberattack believed carried out by the pro-Russia group Killnet	Link
Sep-10	India	Government	24 hours	-	Websites belonging to governments of Assam, Madhya Pradesh, Uttar Pradesh, Gujarat, Punjab and Tamil Nadu were affected.		Link
Sep-11	Sweden	Government	2 days	-	Swedish Government Website www.val.se	The authority's val.se website has been battling severe technical problems as a result of the attacks	Link

Date of attack	Country	Vertical	Duration of Attack	Downtime	Companies affected	Comments	Press
Sep-11	Sweden	Media	1 hour	1 hour	Bonnier News	Several news sites within Bonnier News, including Dagens Nyheter, were hit an attack. Several websites stopped working during the vote count in the parliamentary election	Link
Sep-14	United States	Gaming	3 hours	3 hrs & 11 mins	Blizzard Entertainment	Blizzard under DDoS attack, with BattleNet login attempts affecting WoW, Overwatch, Hearthstone, and more	Link
Sep-15	India	Media	24 hours	-	Blitz Newspaper	There have been over 658.04 million attacks just within 24 hours	Link
Sep-16	Ukraine	Banking	-	-	Monobank	-	Link
Sep-21	Iran	Banking	-	30 minutes	Iran Central Bank	-	Link
Sep-25	Ireland	Gaming/ Gambling	-	18 Hours	Pokerstars Company is Flutter Entertainment	-	Link