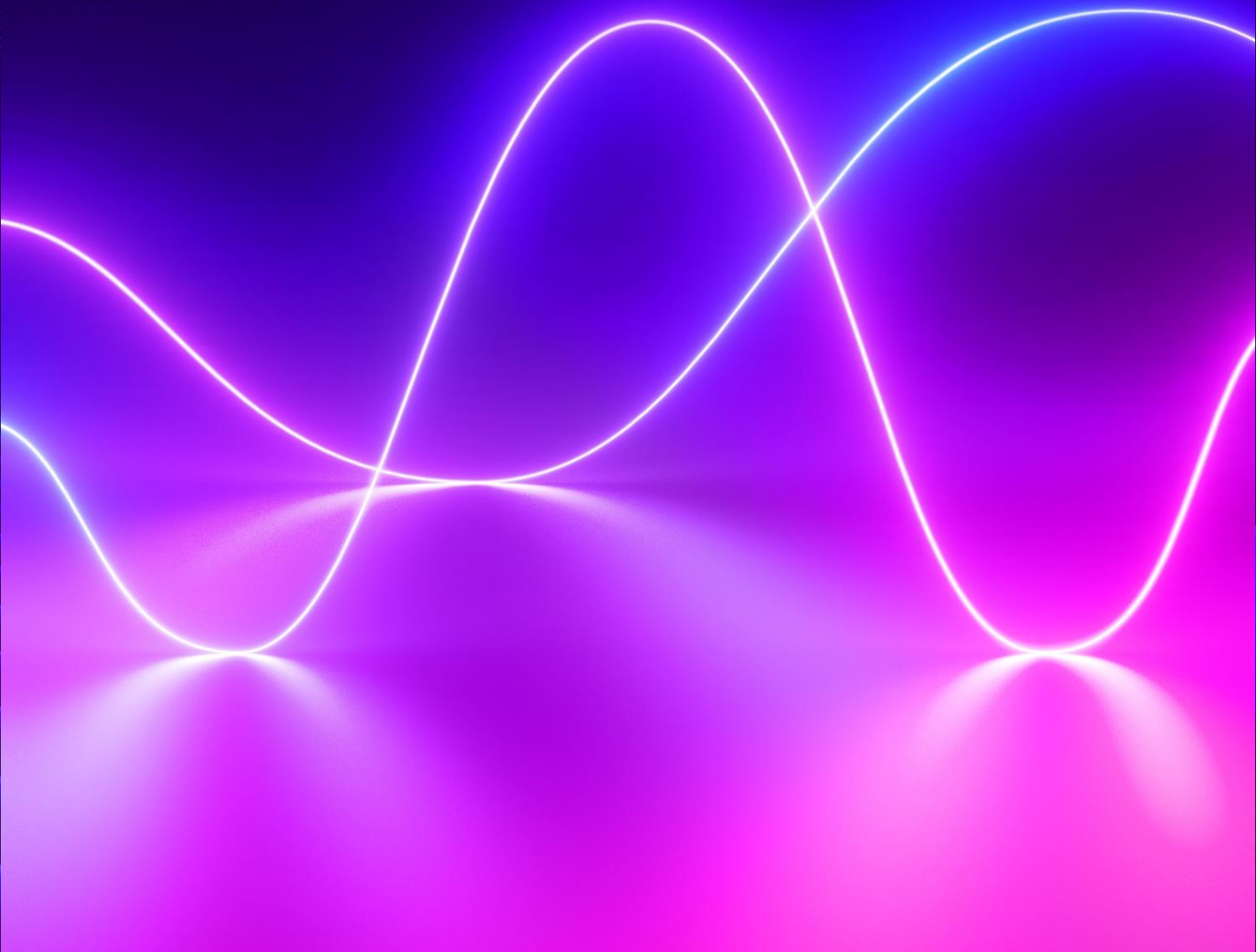
MAZEBOLT

DDoS Attack Round-up

SEPTEMBER 2023 REPORT



Autumn is here, but DDoS causes a wildfire

September of 2023 saw DDoS attackers resuming their criminal operations, after what seemed to be a summer vacation. Several high-profile DDoS attacks severely damaged operations across many sectors, including the Police in India, Transportation in New Zealand and Finland, and Aviation in France and Russia. The gaming industry saw its share of disruptions and downtime as well, with one specific major attack on Bungie's "Destiny 2" - one of the most popular and anticipated games of recent times.

Was the game launch destined to crash?

"Destiny 2" was crippled by a slew of devastating DDoS attacks that shut the game down several times in the span of over a week. Bungie, the game's developer, was not able to handle the situation and admitted that most of the "technical difficulties" gamers experienced were the direct result of DDoS attacks. Players were struggling to remain connected, and some high-profile gamers have publicly called the game "broken", reporting that they're unable to carry out any actions in the game - even simple ones like opening doors.

The reputational damage for Bungie may be enormous, and it is too soon to determine the scope of the overall financial damage. What is clear is that the only reason the game went down is misconfigurations in the DDoS protections deployed - and the only way to identify DDoS vulnerabilities is to continuously and non-disruptively test the DDoS security posture. That was also the major conclusion and recommendation that was given to Canadian organizations by the government, several times in September, following the unprecedented slew of DDoS attacks that hit the country.

Canada took most of the DDoS heat

A critical mass of politically motivated DDoS attacks has crippled many Canadian organizations in September, including government agencies, businesses, and educational institutions. The attacks were widespread and caused significant disruptions, highlighting the growing threat of DDoS attacks to Canadian organizations.

Several Canadian provinces and territories' websites and online services were shut down - including The Quebec government, PEI, Yukon, Nunavut, Saskatchewan, and Manitoba. Other major organizations that were hit were the Manitoba Health Department, Quebec's Treasury Board, Securities Regulator, and the Economy Department in addition to Investissement Quebec (a provincially run investment fund) and the Court of King's Bench online registry.

The first wave of these DDoS attacks, lasting from September 11th to the 17th, was carried out by NoName057(16), the infamous state-sponsored Russian threat actor, that has been wreaking havoc in the last few months. This attack, like others before it, was presumably launched because of Canada's support of Ukraine. But the second wave proved to be no less devastating.

On September 23rd, a second wave of politically-motivated DDoS attacks campaign was launched, this time carried out by the "Indian Cyber Force", a hacker group presumed to be linked to NoName057(16). The attackers referred to Prime Minister Justin Trudeau, who disclosed credible claims that India was involved and perhaps responsible for the death of Sikh separatist activist Hardeep Singh Nijjar.

This second wave included successful attacks on financial and medical organizations, the website of the House of Commons, the Canadian Armed Forces website, the Elections Canada portal (Elections Canada was down for a few minutes), in addition to websites belonging to Canadian small enterprises, such as restaurants and medical clinics.

“This incident is especially concerning,” said Brett Callow, a B.C.-based threat analyst. “It’s the first time I can recall a DDoS attack on a Canadian organization impacting more than its website, and these attacks are trivial to conduct and very easy to repeat.” he concluded.

The Canadian Center for Cyber Security has published official recommendations following the attacks, encouraging organizations to adopt the guidelines and steps recommended by the American Cybersecurity and Infrastructure Security Agency (CISA).

CISA highlights the importance of properly configured DDoS protection layers to gain effective automated DDoS protection and highly recommends always considering automated protections, and not relying on manual intervention that leads to damaging SLAs and causes online service outages.

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
September 1	France	Aviation	24 Hour attack: 12 Hours Downtime	The website of Charles de Gaulles airport in Paris	**NA**	Link	#OpFrance - Dark Storm (state-backed Russian cybercriminals)
September 1	Germany	Finance	96 Hour attack: 72 Hours ongoing downtime	The German Federal Financial Supervisory Authority (BaFin)	**3Mil USD**	Link	Unknown - suspcected pro-Russian hacktivists
September 1	Austria	Media	48 Hour attack: 12 Hours ongoing downtime	The International Press Institute	**NA**	Link	IPI said evidence suggests the same attacker that has been targeting independent media in Hungary is also responsible for the attack on IPI - HANO.
September 6	Austria	Media	96 Hour attack: 72 Hours ongoing downtime	The International Press Institute	**NA**	Link	IPI said evidence suggests the same attacker that has been targeting independent media in Hungary is also responsible for the attack on IPI - HANO.

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
September 8	South Korea	Gaming	36 Hour attack: 12 Hours ongoing downtime	Ironmace - "Dark and Darker"	**NA**	Link	Unknown
September 9	India	Infrastructure	1 Hour	The Delhi Police and the Mumbai police websites	**NA**	Link	Pro Pakistan actor: "Insane PK"
September 11	Canada	Government	48 Hour attack: 12 Hours ongoing downtime	several Canadian provinces and territories — including PEI, Yukon, Nunavut, Saskatchewan, The Quebec government, and Manitoba. The attack also impacted departmental websites such as Manitoba Health as well as the Court of King's Bench online registry. Air Canada has confirmed that it had experienced a security breach that allowed the threat actor to obtain personal information of some employees and certain records.	**NA**	Link	Suspected to be NoName057(16) - State Sponsored by Russia
September 17	Canada	Government	3 Hour attack: 1 hour downtime	The Canada Border Services Agency (CBSA): Airport check-in kiosks	**NA**	Link	NoName057(16) - State Sponsored by Russia

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
September 17	USA	Gaming	48 Hours attack: 10 hours downtime	GGPoker - The world's biggest poker site	**NA**	Link	Unknown
September 18	Finland	Transportation	6 Hours attack: 3 hours downtime	The transport and communications agency Traficom	**NA**	Link	NoName057(16) - State Sponsored by Russia
September 18	Israel	Medical	6 Hours attack: 3 hours downtime	Kfar Shaul psychiatric hospital	**NA**	Link	Unknown
September 18	Israel	Media	3 Hour attack: 1 hour downtime	Two radio websites were offline: 103fm and Galey Israel	**NA**		Unknown
September 19	USA	Gaming	96 Hours attack: 48 hours ongoing downtime	The Destiny 2 Game	**2.5Mil USD**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
September 23	Canada	Finance	6 Hours attack: 2 hours downtime	Moneris, Canadian payment processing firm	**200K USD**	Link	Indian Cyber Force, presumed to be linked to NoName057(16)
September 24	Canada	Government	96 Hours attack: 24 hours ongoing downtime	The website of the House of Commons	**NA**	Link	Indian Cyber Force, presumed to be linked to NoName057(16)
September 26	Russia	Aviation	96 Hours attack: 72 hours ongoing downtime	Several of Russia's airline carriers, such as Aeroflot, Pobeda, Azur Air, and Rossiya. Also, the Leonardo airport check-in system.	**2.2Mil USD**	Link	Ukraine's IT Army
September 26	USA	Social Media	6 Hours attack: 3 hours downtime	Discord	**NA**	Link	Unknown
September 26	Canada	Medical	6 Hours attack: 3 hours downtime	Ottawa Hospital's website	**NA**	Link	Indian Cyber Force, presumed to be linked to NoName057(16)

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
September 24	Canada	Government	96 Hours attack: 24 hours ongoing downtime	The website of the House of Commons	**NA**	Link	Indian Cyber Force, presumed to be linked to NoName057(16)
September 27	Canada	Government	6 Hours attack: 3 hours downtime	The Canadian Armed Forces website and the Elections Canada portal (Elections Canada was down for a few minutes). Also, websites belonging to Canadian small enterprises, such as restaurants and medical clinics.	**NA**	Link	Indian Cyber Force, presumed to be linked to NoName057(16)
September 27	New Zealand	Transportation	3 Hours attack: 1.5 hours downtime	Auckland Transport's website, AT Mobile & AT Park apps, website, Journey Planner, and public information displays.	**300K USD**	Link	Medusa, possibly Pro-Russia