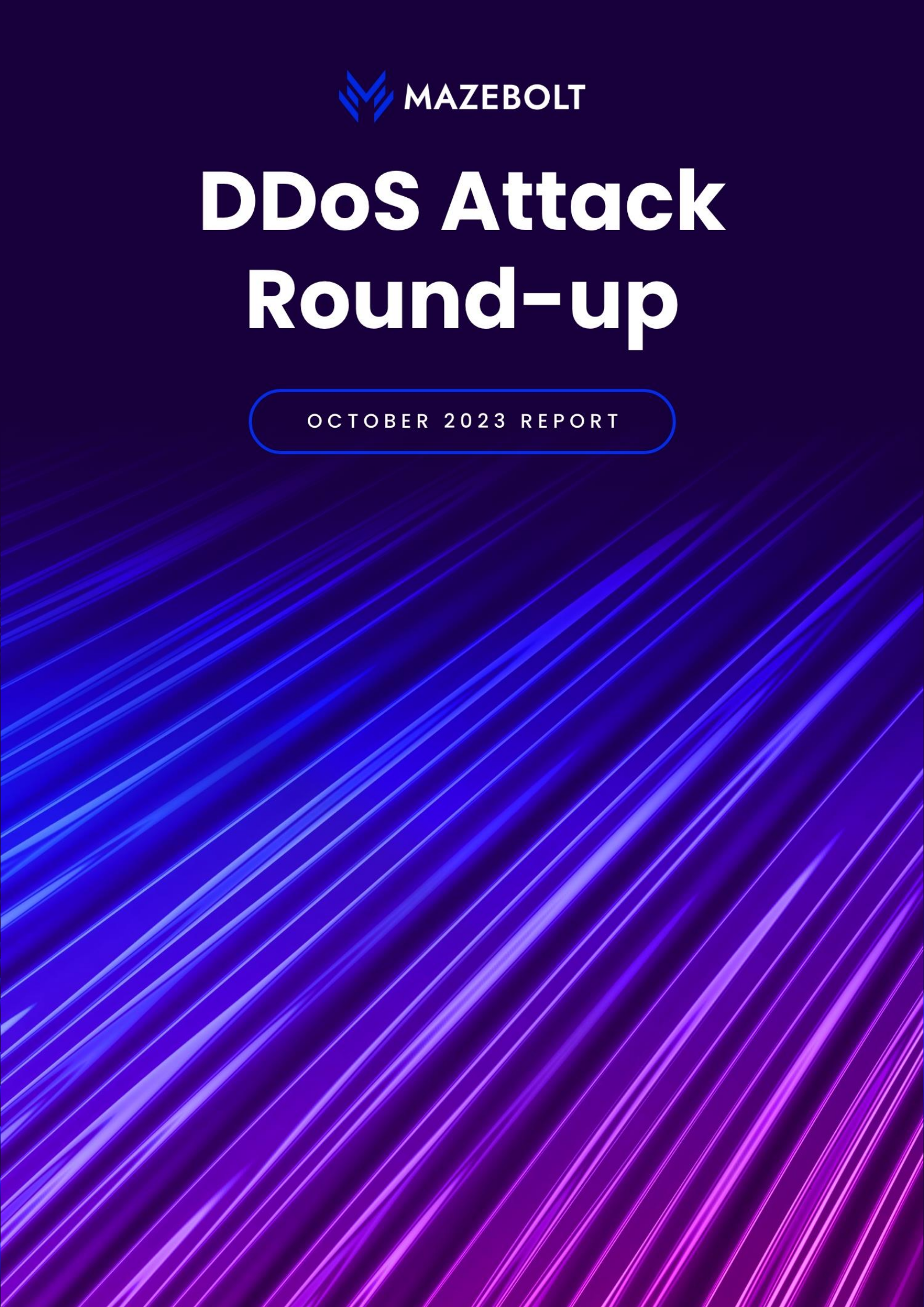
MAZEBOLT

DDoS Attack Round-up

OCTOBER 2023 REPORT



DDoS is in the middle of the Israel/Gaza Frontline

The month of October 2023 opened with a slew of DDoS attacks targeting governmental institutions in leading countries. Starting with the British Royal Family's website, followed by a complex attack on Australian governmental services, and ending with an attack on Spain. All of these attacks were executed by pro-Russian groups, revolving around the attacked countries' involvement with the Russia/Ukraine conflict.

To be honest, here at MazeBolt, we thought this monthly attack roundup would revolve around this issue yet again, as it seems governments are still not accepting the facts about DDoS protection misconfigurations that lead to successful and damaging DDoS attacks. We thought we would talk about that, and about the **gaming industry's challenges with DDoS security**, following yet another successful attack on Ironmace. Or maybe continue the discussion about the complex relationship between the free press and DDos threat actors, following several attacks on press outlets.

We never imagined our main focus this month would be on Israel and Gaza, following a barbaric terror attack on Israel, and an official declaration of war. But life is what happens when you're busy making plans, and we at MazeBolt are committed to providing the most innovative DDoS security solutions, information, and best practices. So, despite the pain, we carry on with our goals and missions.

Sadly, when it comes to cyber-warfare related to the Israel/Gaza war, there's a lot to discuss, and it mostly has to do with DDoS attacks. Since the attack on October 7th, Israel has been experiencing a barrage of DDoS attacks, launched by more than 10 different threat actors. It seems like a coalition was formed, aiming to disrupt Israel's infrastructure by any means possible. On the other hand, several pro-Israel hacktivists have engaged in similar actions, shutting down Palestinian-related outlets. Our report details all the attacks that were made public and officially confirmed, and it is also recommended to follow the following outline of events to get a grasp on how sophisticated DDoS threat actors can get when they share a common goal.

On October 6th, "Cyber Av3ngers" claimed responsibility for hacking the Noga Independent Systems Operator and launching DDoS attacks. While never confirmed to be successful, this event marks the beginning of cyber activity related to the ongoing conflict. On October 7th, within an hour of the 5000-missile attack on Israeli civilians by Hamas, Anonymous Sudan launched DDOS attacks on all the alert applications used for notifying citizens about incoming rockets. On October 8th, the Russian hacker group 'Killnet' claimed responsibility for shutting down the Israeli government's site - but in all likelihood, it was a self-restricting move to geo-block access to protect the country's critical services.

Later that day, Anonymous Sudan attacked The Jerusalem Post's website (the leading English-written press outlet in Israel), causing it to go offline for almost 2 days. On the opposite side, several pro-Israel hacktivists shut down Palestinian-related outlets, such as the Palestinian government websites, the websites of Hamas, and the Islamic University of Gaza.

In the following days, the cyber-war escalated, as various pro-Israel and pro-Hamas hacker groups engaged in cyber activities, shutting down websites and targeting infrastructure, mostly through DDoS attacks. This includes involving citizens willingly adding their IoT devices to botnets, aiming to disrupt as many services as possible. On October 16th, amidst other cyber incidents, Israeli news websites "All Israel News" and "Abu AliExpress" were targeted by "YourAnon T13x" with DDoS attacks. although not officially confirmed, it seems like the sites were indeed down for several minutes.

Some of the threat actors decided to title their efforts as "OpIsrael2". Although trying to escalate the DDoS attacks as the fighting progressed, Israel increased its ground operation and the last remaining internet and mobile connections in Gaze went dark. As of writing this report, many DDoS threat actors are still trying to shut down critical online services in Israel, with little success, as the Israeli government is known for its heavy investments in DDoS security. Among these well-known threat actors are Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army, and others.

We hope this war ends soon and for peaceful days ahead. As we've published before, many organizations are currently understaffed due to different reasons including military reserve duties and personal time off. During these challenging times, everyone can do something to help someone. We, at MazeBolt, extend our hands to any organization in Israel and abroad that is suffering from a DDoS attack related to the current conflict with Hamas. Any organization that requires assistance can contact us at support@mazebolt.com - we are here for you.

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 1	UK	Government	3 hours attack 1 hour downtime	The Royal Family's official website	**NA**	Link	KillNet, Russian Hacktivist group
October 5	Australia	Government	8 Hours attack 5 hours downtime	the Department of Home Affairs and Administrative Appeals Tribunal websites in response to a decision to provide the Slinger "drone killer system" to Kyiv.	**NA**	Link	NoName057(16) - State Sponsored by Russia
October 6	Spain	Government	3 hours attack 1 hour downtime	several public and private websites, including in the city of Granada where an EU summit is taking place, The Granada Bus service	**NA**	Link	NoName057(16) - State Sponsored by Russia
October 6	US	Social Media/ Financial	12 Hours attack 6 hours downtime	Stars Arena, a social platform backed by Avalanche's Contract Chain - The DDoS attack was a cover for a financial hack	**4Mil USD**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 7	Israel	Government, Infrastructure - "OpIsrael2"	Unconfirmed	Unconfirmed	**NA**	Link	Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army and others
October 8	Israel	Press - "OpIsrael2"	48 Hours attack 16 hours intermittent downtime	The Jerusalem Post	**50K USD**	Link	Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army and others
October 8	Israel	Government	1 Hour attack 1 hour downtime	Shin Bet, the Israeli Homeland Security	**NA**	Link	KillNet, Russian Hacktivist group
October 8	South Korea	Gaming	48 Hour attack: 24 Hours intermittent downtime	Ironmace – "Dark and Darker"	**NA**	Link	Unknown

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 8	The Palestinian Authority	Government	24 Hours attack 12 hours downtime	The Palestinian government websites, the websites of Hamas and the Islamic University of Gaza.	**NA**	Link	The Indian Cyber Force, and also TeamHDP
October 9	The Palestinian Authority	Government	24 Hours attack 12 hours downtime	Palestinian telecommunications company, the National Bank's website, a government webmail service, and the official Hamas website.	**NA**	Link	The Indian Cyber Force
October 12	Israel	NPO	12 Hours attack 6 hours downtime	United Hatzalah - Jerusalem-based nonprofit which provides emergency medical services	**NA**	Link	Mysterious Team Bangladesh, Anonymous Sudan, Insane Pakistan, Garnesia Team, Moroccan Black Cyber Army and others
October 12	The Palestinian Authority	NPO	12 Hours attack 6 hours downtime	Medical Aid for Palestinians (MAP), a British charity helping with emergency relief	**NA**	Link	Unknown
October 12	Belgium	Government	24 Hours attack 6 intermitten t hours downtime	Websites of the Royal Palace, the Prime Minister and the Parliament of Brussels: presumably in response to Volodymyr Zelenskyy's visit to Belgium and its decision to deliver F-16 fighter jets to Ukraine.	**NA**	Link	Unknown but pro-Russian

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 13	Iran	Government	24 Hours attack 12 hours downtime	Mojahedin.org website	**NA**	Link	Ministry of Intelligence and the IRGC, under the command of Khamenei
October 14	Guatemala	Government	24 Hours attack 12 hours intermittent downtime	Webpages for Guatemala's judicial branch, Department of Agriculture and the General Secretary of the president, and more – in support of Indigenous organizations in the country	**NA**	Link	Anonymous
October 14	USA	Healthcare	12 Hours attack Unknown hours intermittent downtime	Major U.S. healthcare solutions provider Henry Schein	**3.3Mil USD**	Link	Unknown
October 22	USA	Entertainment	4 Hours attack 2 hours downtime	Deezer	**150K USD**	Link	Unknown
October 22	Australia	Sports	2 Hours attack 1 Hour downtime	West Australian Optus Stadium	**NA**	Link	Team Insane Pakistan

Date of attack	Country	Vertical	Downtime	Companies Affected	Estimated Damage	Press	Threat Actor + Affiliation
October 24	Czech Republic	Government	4 Hours attack 2 Hours downtime	The websites of the Czech Ministry of the Interior and police force, website of the Crimea Platform international summit	**NA**	Link	Unknown – but presumed from Russia
October 27	Russia	Telecoms	8 Hours attack 4 Hours downtime	Three Russian internet providers — Miranda-media, Krimtelekom, and MirTelekom	**NA**	Link	Ukrainian IT Army
October 31	USA	Press	3 Hours attack 3 Hours downtime	AP - Associated Press, one of the world's best-known news organizations	**NA**	Link	Anonymous Sudan