Radware Cybersecurity Advisory

Hacktivism Unveiled, India

Insights into the footprints of hacktivists

May 17, 2023

In the last three months, hacktivists have claimed 480 DDoS attacks targeting Indian websites, making India the most targeted country for hacktivist groups tracked by our Threat Intelligence team. Hacktivist campaigns targeting India have been on the rise due to negative sentiments spread through social media campaigns.

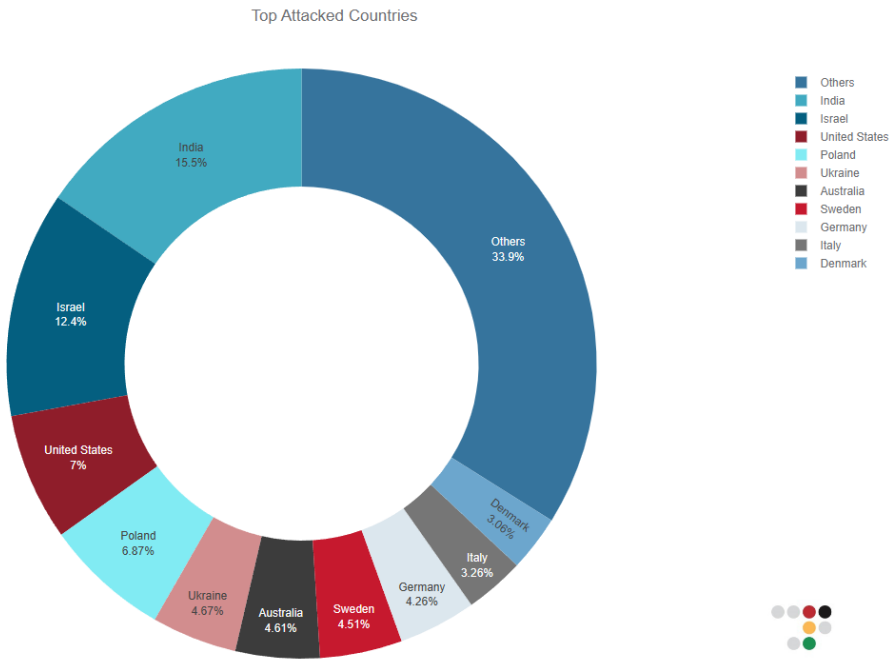

Figure 1: Top targeted countries

Hacktivism

Hacktivism is a complex phenomenon that can be motivated by various factors, including religious and political beliefs. While hacktivists may have different motivations and methods, they all share a desire to use technology to advance their cause and to challenge those they believe are acting against it.

Hacktivists use a variety of tactics to achieve their goals, and the specific tactics they use depend on their motivations and the resources they have at their disposal. Their methods are constantly evolving as new technologies and platforms emerge. While some tactics may be illegal or unethical, hacktivists argue that they use their skills to promote social or political change and hold powerful organizations and governments accountable for their actions.

RELIGIOUS HACKTIVISM

Although politically driven patriotic hacktivists have certainly left an impression since the war in Ukraine started, religious hacktivists have been a constant threat for years—and that did not change because of the war. This year, a new group made headlines when their attacks aligned with pro-Russian hacktivists. Anonymous Sudan, an allegedly Sudan-based pro-Muslim hacktivist group, was announced as a Killnet cluster member by KillMilk. This occurred after the group attacked Sweden and Denmark for the burning of the Quran—outside the Turkish embassy in Stockholm—by the Danish-Swedish right-wing activist Rusmas Paludan. There is still a lot of controversy and confusion surrounding Anonymous Sudan's status as a religiously driven activist group. In a report following the DDoS campaigns that targeted Swedish and Danish websites in February 2023, the security firm Truesec concluded that Anonymous Sudan is a false flag operation by the Russian government, leveraged in an information operation to harm and complicate Sweden's NATO application. After targeting Sweden and Denmark, the pro-Islamic group put its crosshairs on French airports, education, health care and government websites in response to the publishing of a cartoon of the Prophet Muhammed by the French magazine Charly Hebdo several years ago. When the pro-Islamic hacktivist crews Team Insane PK, Eagle Cyber, and Mysterious Team targeted Australia because an Australian fashion label featured models wearing designs with "Allah walks with me" inscribed in Arabic across the fabric, Anonymous Sudan joined the #OpAustralia campaign and started targeting Australian businesses and government websites with DDoS attacks. In April 2023, the group declared India their latest target to sympathize with Indian Muslims under their misperceived Islamic cause. At the time of this writing, Anonymous Sudan was able to create a following of over 30,000 members on its Telegram channel.

HACKTIVIST TACTICS

Some common tactics used by hacktivists:

- **Denial-of-service attacks**: This involves overwhelming a website or online service with traffic, making it unavailable to users. Hacktivist groups use DDoS attacks to disrupt the websites of organizations and governments they oppose. Since the start of the conflict in Ukraine, DDoS attacks have been performed on both sides of the conflict with Ukrainian hackers targeting Russian organizations and pro-Russian hackers targeting any government or organization that might demonstrate support to Ukraine.
- **Website defacements**: Hacktivists may hack into a website and replace its content with their own messages or images. This tactic is often used to express dissent or to raise awareness of a particular issue. Pro-Muslim hacktivists claimed a good number of defacements in recent attacks against Israeli business and government websites during **#OpIsrael** and **#OpsPetir**.
- **Data breaches**: Hacktivists may gain unauthorized access to an organization's computer systems and steal sensitive information, such as personal data or confidential documents. They may then release this information publicly or use it to further their political or religious goals. Over the last few months, pro-

Russian and pro-Muslim hacktivists have claimed a large number of data breaches and credential compromises. While many are most likely to be fake breaches leveraging old and previously stolen documents from prior data leaks, this remains hard to prove, and the sheer volume of claimed breaches makes it impossible to assess the success of the hacktivists.

- **Media campaigns**: Hacktivists may use social platforms like Telegram, Twitter or Facebook and media to spread their message and raise awareness for their cause. They create viral campaigns or use hashtags to amplify their message and reach a wider audience. **DragonForce Malaysia** has proven to be highly effective in their communications by building a community and becoming very proficient in the graphical designs for their operations.

India

Hacktivist campaigns targeting India have been on the rise due to negative sentiments spread through social media campaigns like “Islamophobia_in_India” and “SaveIndianMuslims.” These campaigns often involve the sharing of fake content by people in India and abroad who have strong ideological biases. This fake content provokes hacktivist groups to misunderstand the actual social and political situation in India and take action.

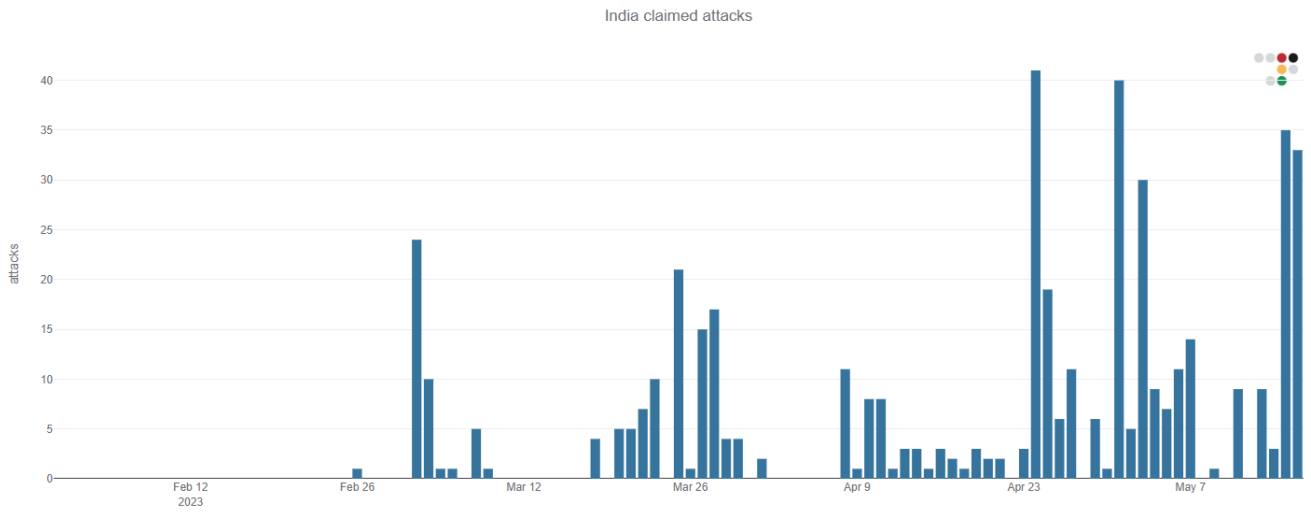

Figure 2: Number of DDoS attacks targeting India claimed by hacktivists per day

One example of such a campaign was the Indian farmer's protest in 2020, which led to the emergence of hacktivist groups like Anonymous India and the Red Rabbit Team. These groups used social media to raise awareness about the protests and launched cyberattacks against individuals and companies they believed were against the movement.

In 2022, there was a series of hacktivist incidents targeting India that lasted for two months. These campaigns were initiated by a prominent hacktivist group called DragonForce Malaysia, under the campaign OpsPatuk. Many other hacktivists who shared the same ideology also participated. The campaign continued under the name OpIndia after DragonForce Malaysia distanced itself from it in June 2022.

Throughout 2022, there were intermittent hacktivist attacks against Indian entities. Then, on February 5, 2023, a group called Team Insane PK restarted the OpIndia campaign on Kashmir Solidarity Day. They launched cyberattacks and leaked documents from the Indian government and private organizations. Since then, they have collaborated with other hacktivists who are also against India.

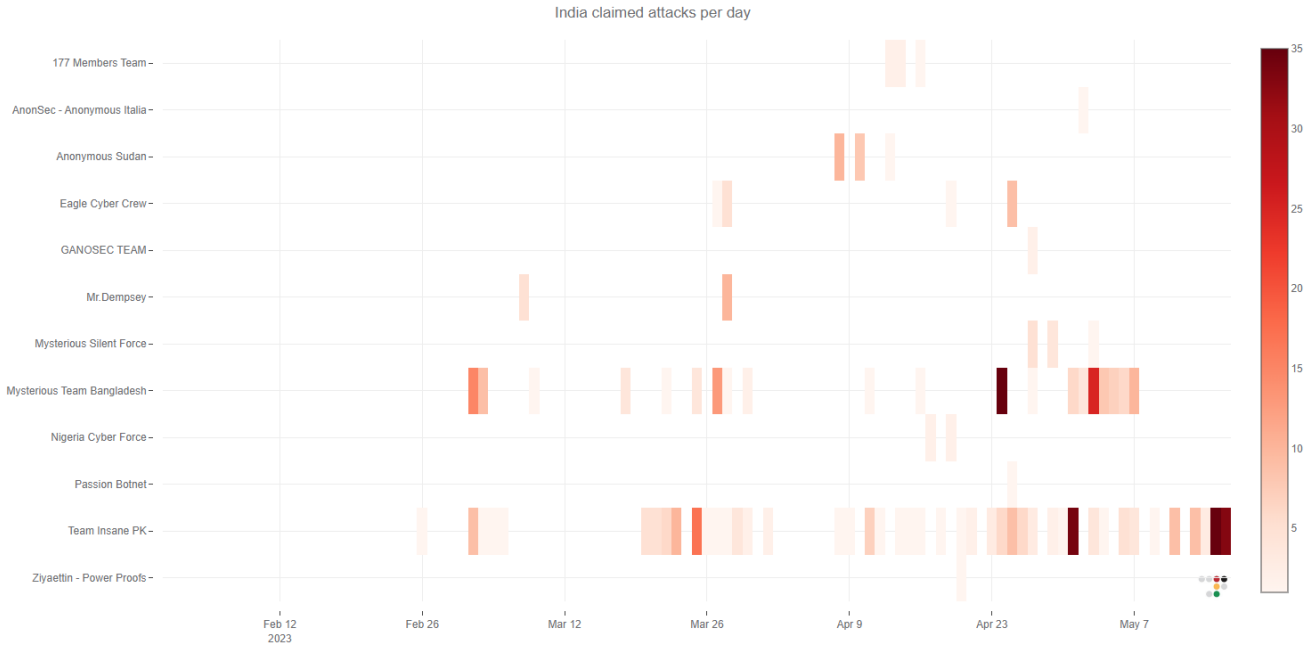

Figure 3: DDoS attacks targeting India claimed by most prominent hacktivist groups

A group of individuals operates Team Insane PK. Two of them are known as Mr Insane and HOAX1337. Besides targeting India, they have also attacked websites in other countries such as the Philippines, Sweden, Afghanistan, Russia, Dominican Republic, Indonesia and Brazil. Interestingly, they have also targeted government websites in Pakistan, using religious reasons to justify their attacks.

In March 2023, another hacktivist group called Mysterious Team Bangladesh started a campaign named "Operation Payback." They launched multiple cyberattacks against Indian websites and publicized their actions on social media and internet messaging channels. This campaign was a response to Indian hacktivists targeting websites in Pakistan, Bangladesh, Indonesia and Malaysia.

Mysterious Team Bangladesh also leaked files from past security breaches. These files included various identification documents like Aadhaar cards, PAN cards, passports, old bank statements, invoices, checkbooks and scanned payment cards. Most of the leaked documents were outdated, but some were still valid. The group has a history of conducting hacktivist campaigns with a pro-Islamic ideology against several countries. They claim to have been active since 2012 and have been involved in previous campaigns like OpIndia, OpsPatuk and OpIsrael.

Other hacktivist groups that supported these campaigns included Ganosec Team, Hacktivist of Garuda, Khalifah Cyber Crew and Eagle Cyber Crew.

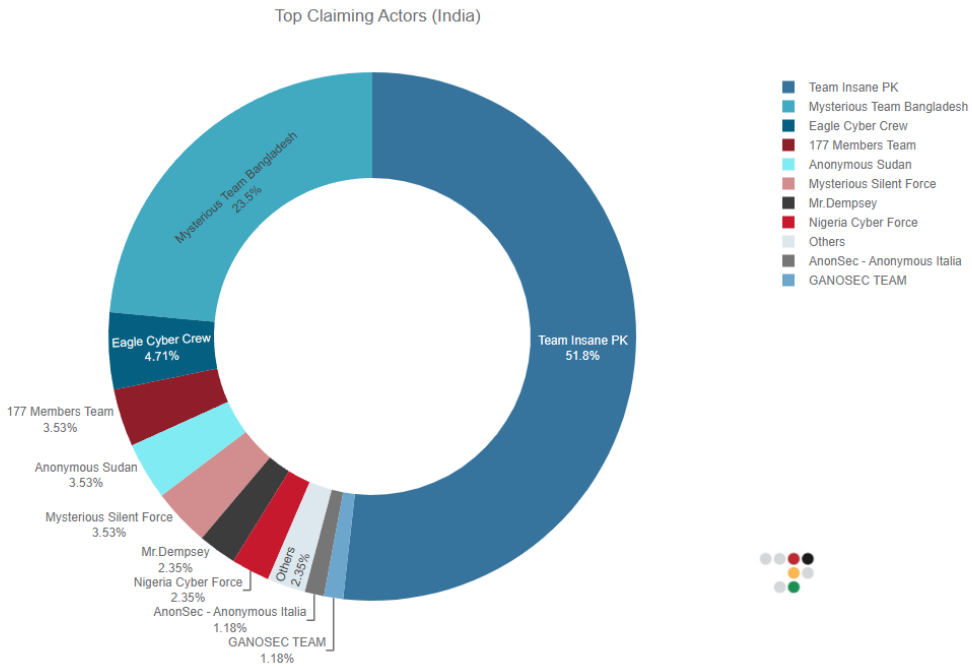

Figure 4: Top claiming hacktivist groups

In March 2023, during Ramadan, Eagle Cyber Crew and eight other groups from Malaysia, Bangladesh, Pakistan, Indonesia, Yemen, Vietnam, Sudan and Palestine launched a campaign called #opsjentik. These groups believed that Indian Muslims were victims of social injustice and carried out cyberattacks against India. They were also involved in the OpIsrael campaign.

Eagle Cyber Crew, claiming to be from Malaysia, created their Telegram channel in December 2022. They identified themselves as part of the "Army of Mahdi" and the "Anti Dajjal Community," referring to figures from Islamic scripture.

On April 19, 2023, Eagle Cyber Crew, along with other hacktivist groups like 4-EXPLOITATION, Khalifah Cyber Crew and Tiger Cyber Crew, started a campaign called OpAbabeel. This campaign was in response to Indian hacktivists leaking data of Muslim citizens. They used tactics like DDoS attacks, defacement and selling compromised databases from India. However, the data samples they shared were actually from a 2020 leak by another threat actor.

In this campaign, their main targets were Indian government entities, the judiciary and educational institutes. They also targeted companies in Mexico, the United States, Ghana and Cyprus.

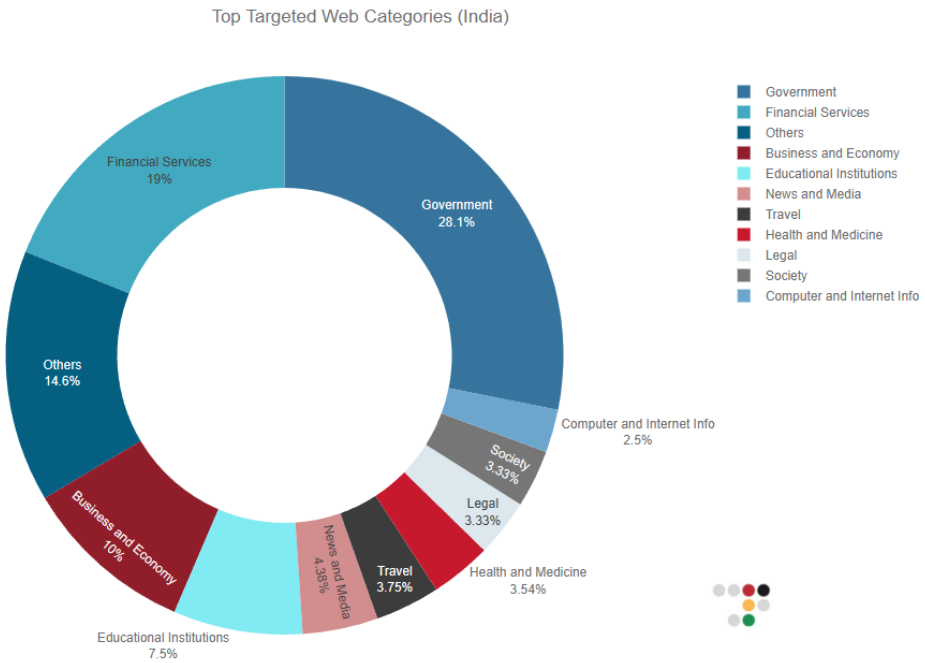

Figure 5: Top targeted website categories

Another campaign called OpIndia2.0 was initiated by Indonesian hacktivist groups VulzSec and Hacktivist of Garuda on April 20, 2023. This campaign was retaliation against attacks on Indonesian government sites by Indian sympathizers. They planned to launch DDoS attacks on 54 entities, mainly government websites of different Indian states. However, they stopped the campaign when approached by a pro-Indian hacktivist group called Kerala Cyber Xtractors. Other groups like GANOSEC TEAM and Team Insane PK continued their attacks despite this truce.

On April 26, 2023, pro-Islamic groups started another campaign called #OpIndia23. This ongoing campaign aims to protest against perceived injustice and prejudice against Indian Muslims. Various hacktivist groups,

including Mysterious Silent Force, DragonForce Malaysia, Mysterious Team Bangladesh, Pakistan Cyber Hunters, AnonGhost and others, are involved in this campaign. They claimed to compromise government websites of Kerala, Rajasthan, Maharashtra, and Jammu and Kashmir, as well as leak related data.

In retaliation to attacks on Indian infrastructure, a few Indian-sympathizing hacktivists emerged from the shadows. They publicized their claims of DDoS on organizations from Bangladesh, Indonesia, Malaysia and Pakistan on social media and their Telegram channels. Among many such small factions, the following groups are leading coordinated waves of attacks: Anonymous India, Mariana's Web, Team UCC Operation, Indian Cyber Mafia, Indian Cyber Force, Team 1-4-1 and Kerala Cyber Xtractors.

Disruptive Web DDoS Attacks

As Radware observed in recent attack campaigns, attackers are leveraging multiple types and vectors as part of a single attack campaign. They're combining both network- and application-layer attack vectors by leveraging improved and new publicly available tools to create sophisticated attacks that hit harder, and sometimes are impossible to detect and mitigate with traditional methods.

Attackers generate new types of HTTPS Flood attacks—also referred to as Web DDoS Tsunami attacks—that are more sophisticated and aggressive. They bypass traditional application protections using sophisticated methodologies, such as randomizing HTTP methods, headers, and cookies, impersonating popular embedded third-party services, proxying IPs, HTTP pipelining and more. Among the application-level attack methods seen in these recent campaigns were HTTPS GET, PUSH and POST request attacks with changing parameters and arguments, orchestrated from cloud-hosted virtual private servers and hiding behind several thousands of daily rotating proxies.

The move towards encrypted attacks and the increase in the scale and sophistication of these attacks raises the bar needed for detection. It renders network-based DDoS mitigation tools and traditional on-prem and cloud-based WAF solutions ineffective against these attacks.

NEW ADVANCED PROTECTION FOR WEB DDOS ATTACKS

As part of its Cloud Application Protection Service, Radware's new Cloud Web DDoS Protection solution is uniquely designed to protect against high-scale, newly emerging Web DDoS Tsunami attacks and provide customers with advanced protection at the scale needed to combat these threats.

Concluding

Over time, hacktivism has become more negative. What began as a way to support social and political change has turned into a harmful method for criminals to push their beliefs, disrupt governments and businesses, and

cause social unrest. In the past year, we've also seen the rise of patriotic and government-backed hacktivism. As hacktivism tactics and beliefs keep changing, public and private organizations and governments must ensure the safety and continuity of their online services and business.

References

1. **Indian Ideology Targeted by Hacktivists: Reprisal Hacktivism Draws More Attacks** by Cyble Research & Intelligence Labs, April 2023
2. **Hacktivism Unveiled, April 2023 Report** by Radware, April 2023
3. **DragonForce Malaysia: OpsPetir** by Radware, April 2023
4. **OpIsrael: A Decade in Review** by Radware, March 2023
5. **OpAustralia & Opsjentik** by Radware, March 2023
6. **DragonForce Malaysia / OpsIndia** by Radware, June 2022
7. **OpsBedil Reloaded 2022 by DragonForce Malaysia** by Radware, April 2022
8. **DragonForce Malaysia OpsBedil** by Radware, July 2021