TACTIC
DISTRIBUTED DENIAL OF SERVICE (DDOS)

A coordinated online effort that brings together vast numbers of people to target a powerful entity's website by flooding it with high levels of data traffic. A powerful means to draw attention to your cause.

CONTRIBUTED BY

Darya Alikhani

Darya is an editor at Beautiful Trouble, a Youth and Multimedia Advisor for ActionAid Myanmar, and an art lover living sometimes in Cyprus, sometimes in Myanmar, sometimes online. She can usually be found in pursuit of interesting objects and absurd ideas.

"TO BE TRULY EFFECTIVE AS A PRESSURE TACTIC, ANY DDOS ACTION NEEDS TO BE EMBEDDED WITHIN A LARGER CAMPAIGN OF PUBLICITY AND MESSAGING."

"Pretty things will swarm you like that, like your heart was a hive of electric bees."
—Katherine Dunn

In January 2019, following a week of protests against raised fuel prices and high living costs, Zimbabweans found themselves facing a government-ordered internet shutdown. Shortly afterwards, the hacktivist collective Anonymous launched #OpZimbabwe, a series of distributed denial of service (DDoS) attacks that took down at least 73 government websites, severely impacting banking and other systems. A similar operation, #OpSudan, also staged a series of attacks against Sudanese government websites, using Twitter to present the Transitional Military Council with an ultimatum: restore internet access immediately or your cyber infrastructure will suffer (see: TACTIC: Hashtag campaign).

Distributed denial of service, or DDoS, is a coordinated swarm that interrupts the operation of powerful targets by flooding their sites with high levels of data traffic. If successful, access to targeted websites is restricted and services are temporarily disabled.

At its simplest, this involves individuals working together to continuously reload a website, thereby aggregating their digital 'requests' for access to the site to overwhelm the target website's resources, forcing it to shut down. The fact that it is distributed, with a large enough number of participants from various locations, makes it extremely difficult to trace back to any one or more individuals.

POTENTIAL RISKS

It's not exactly legal...

Aside from the risk and implications for individual participants of getting caught, engaging in DDoS can also be used to discredit the movement on legal grounds.

Choose wisely, be wary of collateral damage

An important consideration for DDoS targeting corporate entities is the potential for unintended effects on the public. For instance, if your target is a profiteering pharmaceutical company, a temporary disruption may impact distribution or access to medication for those in need. Focusing on taking down the marketing division of the company for example, is one way to set-back your target, while leaving bystanders unharmed.

A successful DDoS can take down websites and servers for hours at a time, which can cause significant loss of revenue for big businesses or reputational damage to government institutions and private companies (see: METHODOLOGY: Points of intervention).

Over the last few decades, DDoS has been frequently used as a tool for online protest. It's not surprising why: Firstly, participants don't have to be physically present to engage. Unlimited numbers can take part globally. Secondly, it requires very little technical skill; anyone with a digital device and an internet connection can join or offer up their devices as part of the action while they go about their business elsewhere. Thirdly, it's low cost with the potential for big impact.

In 1994, the German government began a program to deport asylum seekers and refugees, using Lufthansa flights. The Deportation Class Action campaign, initiated by the Electronic Disturbance Theatre (EDT), coordinated a DDoS with 13,000 online participants, rendering the Lufthansa website inaccessible for short periods of time. The action was carried out alongside stockholder meetings, press releases, and other physical actions, and resulted in drawing enough public attention to the airline's business that it stopped allowing its flights to be used for deportation purposes (see: PRINCIPLE: Put your target in a decision dilemma).

In and of itself, the Lufthansa action may not have yielded enough pressure to change corporate behaviour, but, when carried out as part of a multi-pronged public campaign focused on a company seeking to avoid negative press, the pressure proved enough to secure victory (see: PRINCIPLE: Create online-offline synergy). To be truly effective as a pressure tactic, any DDoS action needs to be embedded within a larger campaign of publicity and messaging. If the motivations and cause for which you are demanding action are not clearly communicated, simply putting a website out of service temporarily can easily be explained away as a mere technical glitch.

More recently, tactics for carrying out a DDoS have had to significantly evolve to effectively pressure large and powerful targets, which have invested heavily in their digital defenses. As a result, the use of botnets, traffic multipliers, automated tools and other exploits to 'increase' numbers — and by extension the technical power of DDoS — are becoming commonplace. Criminal networks have also seized on these tools to extort powerful targets, resulting in many governments treating DDoS "cybercrime" as a felony. This can pose both ethical and legal dilemmas for organizers who may opt to use tools that do not reflect the numbers of real-life participants to the action. What's worse, a group may find their own online platforms being targeted by large actors with big resources, or find cybercrime law being weaponized against their just cause.

DDoS reflects the double-edged nature of information communication technologies: they can be employed as a tool of censorship to silence public opposition, and they can be used to

Using traffic multipliers and exploits to maximize impact

Similar to a sit-in, street protests and other crowd-based tactics, it is the large numbers of willing participants that can lend DDoS actions their political and ethical legitimacy. The use of traffic multipliers and exploits, while tempting in their capacity to cause significant disruption, greatly increases the technical and legal risks of the action.

You could be on the receiving end of a bigger, badder DDoS!

Today, anyone with significant resources can pay for a DDoS. That includes cybercriminals, politically motivated groups, and governments. Picture a violent street protest organized by a majority party to stifle opposition through a show of force(see: THEORY: Baltajiah [thugs]), or an election monitoring website being 'unavailable' to provide information during the voting process. The limited traceability of a DDoS action makes it a highly attractive tool to silence opposition websites (anywhere in the world) with plausible deniability.

RELATED TOOLS

Tactics

- Blockade
- Distributed action

Principles

- Choose tactics that support your strategy
- Choose your target wisely
- Put your target in a decision dilemma
- Simple rules can have grand results
- Take risks, but take care

challenge and resist that censorship (see: TACTIC: Hashtag hijack). DDoS also carries a unique potential for mass participation, offering large numbers of people a meaningful way to climb the ladder of engagement (see: TACTIC: Distributed action).

If attempting a DDoS, it is vital that participants are informed and prepared for the risks they may face individually, as well as the implications for the campaign — including the legal risks participation may entail (see: PRINCIPLE: Take risks, but take care) (see: PRINCIPLE: Escalate strategically). Anonymity is never guaranteed, and the legal risks, as in any act of civil disobedience, should not be entered into lightly.

LEARN MORE

The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet, by Molly Sauter
Bloomsbury, 2014
https://www.bloomsbury.com/us/coming-swarm-9781623568221/

Theories

- Baltajiah (thugs)

Methodologies

- Points of intervention

TAGS

Digital organizing,