Case study: Distributed Denial of Service attacks (DDoS)

June 2020

THE ENGINE ROOM

Contents

Introduction

The purpose of this case study is to illustrate the consequences of digital attacks against human rights and alternative media organisations, while recommending how such organisations–and practitioners from all backgrounds supporting them–may mitigate digital attacks.

This case study is one of three, which were prioritised based on a review of recent digital attacks and identification of which were most common. In creating these case studies, we reviewed documentation of community events, community research, interviews with digital security practitioners and responders conducted by The Engine Room, and incident trackers from the MONITOR regional support leads from April 2019 - March 2020. Further desk-based research was conducted on the specific type of attack to supplement each case study.

Description of attack

“A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic”.[1]

A DDoS attack remains one of the most effective ways of forcing a website to shut down. In DDoS attacks, sites (or specific pages) become inundated by an overwhelming load of requests, making it so that the server on which the website is hosted is no longer able to accept more requests.

Attacks on Philippine alternative media organisations

One relevant example of this type of attack was launched on alternative media organisations in the Philippines between late 2018 and early 2019. Some of the media organisations involved were: Bulatlat, Kodao Productions, Pinoy Weekly and the National Union of Journalists (NUJP) website[2].

According to a statement from AlterMidya, the attacks began in early December 2018 and by December 26, all of the sites were inaccessible.[3] The DDoS attacks continued until February 5 2019, and, as the NUJP reported later, attacks to their website were repeated on February 11, 2019.

While these sites had been attacked individually in the past, the scale and the coordination of these DDoS attacks had not been seen before.

The media organisations that were targeted believe that these attacks were meant to silence dissent against the Philippine President Rodrigo Duterte and his administration.

---

1 "What is a DSoS Attack?" *Cloudflare* https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Date Accessed: 06 April 2020)

2 “DDoS attacks on NUJP, alternative media continue” https://nujp.org/headlines/ddos-attacks-on-nujp-alternative-media-continue/

3 "Alternative Media Under Seige" *AlterMidya* https://www.altermidya.net/alternative-media-under-siege/ 28 December 2018 (Date Accessed: 06 April 2020)

Based on what was published in AlterMidya, the attacks against Bulatlat in December 2018 came after they reported on the anniversary of the Communist Party of the Philippines. According to Bulatlat, the attacks in January 2019 started when they published two reports: one on how the Philippine government is abandoning its children by lowering the minimum age of criminal responsibility and another on the release of peace activist, Rafael Baylosis.[4]

Based on an NUJP report, the most requested URL path for the attacks on 11 February 2019 was *https://nujp.org/?s=duterte*, a page that appears when keyword "Duterte" is searched on the website[5]. The NUJP mentioned in a report on February 11 that "like the previous attack, we strongly believe this is part of an orchestrated campaign to silence critical outfits and organizations that has also targeted alternative news sites"[6].

Since the end of January 2019, some of the attacked media organisations progressively migrated their websites to VirtualRoad (https://www.qurium.org/secure-hosting/), Qurium Media Foundation's secure web hosting service for independent online news outlets and human rights organizations under threat. Bulatlat in particular, did so on January 25 - in the middle of attacks. This allowed Qurium to monitor and investigate the DDoS attacks against these websites, particularly those against Bulatlat, which had been hosted by Cloudflare prior to the attacks.[7]

Cloudflare assisted Bulatlat with DDoS mitigation when the first wave of attacks began on December 26th 2018, but were unable to prevent the campaign from shutting down the website in January of the following year.[8]

The forensics reports from Qurium allowed the media companies to file a lawsuit against the IT companies implicated in the DDoS attacks.[9]

For more information about this incident, take a look at resources put out by both Qurium and Bulatlat: Forensic investigation made by Qurium Media Foundation on the Philippine Cyber-attack and What you need to know about the on-going cyber-attacks vs alternative news Bulatlat (07 February 2019).

In this case, the DDoS attacks occurred within the context of President Rodrigo Duterte's actions against press freedom in the Philippines–which included threats against Rappler.com and its founder,

---

4 Ellao, Janess Ann J. *Bulatlat* "What You Need to Know about the On-going Cyber Attacks vs Alternative News Bulatlat" https://www.bulatlat.com/2019/02/07/what-you-need-to-know-about-the-ongoing-cyber-attacks-vs-alternative-news-bulatlat/ 07 February 2019 (Date accessed: 06 April 2020)

5 "DDoS attacks on NUJP, alternative media continue" *National Union of Journalists* https://nujp.org/headlines/ddos-attacks-on-nujp-alternative-media-continue/ 11 February 2019 (Accessed: 06 April 2020)

6 DDoS attacks on NUJP, alternative media continue https://nujp.org/headlines/ddos-attacks-on-nujp-alternative-media-continue/

7 https://www.bulatlat.com/2019/02/07/what-you-need-to-know-about-the-ongoing-cyber-attacks-vs-alternative-news-bulatlat/

8 "Attributing attacks against media and human rights websites in the Philippines" *Qurium Media Foundation* https://www.qurium.org/alerts/philippines/attributing-the-attacks-against-media-human-rigths-philippines/ 29 March 2019 (Date accessed: 06 April 2020)

9 Ellao, Janess Ann J. "A Second Look at the Charges Files vs IT Companies Over News Sites Cyberattacks" *Bulatlat.com* https://www.bulatlat.com/2019/04/05/a-second-look-at-the-charges-filed-vs-it-companies-over-news-sites-cyberattacks/ 5 April 2019 (Date accessed: 06 April 2020)

Maria Ressa beginning in 2017[10] – and alongside an unprecedented number of threats against journalists and media organisations in the Philippines:

“Separately and together, these 85 cases have made the practice of journalism an even more dangerous endeavor under Duterte.

From June 30, 2016 to May 1, 2018, these cases include the killing of 9 journalists, 16 libel cases, 14 cases of online harassment, 11 death threats, 6 slay attempts, 6 cases of harassment, 5 cases of intimidation, 4 cases of website attack, revoked registration or denied franchise renewal, verbal abuse, strafing, and police surveillance of journalists and media agencies.”[11]

Zoom-in: Using a forensics report to file charges against IT companies over news sites cyberattacks

On March 29, 2019, the group of Philippine alternative media outlets that reported the DDoS attacks filed a civil complaint before a Quezon City Regional Trial Court against two IT companies: IP Converge and Suniway Group of Companies.

As shared by one of the media outlets, Bulatlat,[12] Qurium Media Foundation’s forensics report revealed that the IP addresses were exposed when the alleged attackers committed a mistake of visiting the website under attack without turning on their hidden virtual private network and when another visited the website through a Samsung phone.

Qurium noticed suspicious “extra hops” in the traffic traces, which they later discovered as a traffic tunnel between Hong Kong and Manila. The said traffic tunnel infrastructure, which diverts the origin of attacks, was owned by Suniway.

Qurium later on reached out to IP Converge, informing them that they had received reports about an attack coming from their network. Despite several emails, by the time the news report was published by mainstream media (April 2019), IP Converge hadn’t acknowledged or responded to these messages.

Meanwhile, Qurium said in its report that the attacker could easily be identified by Suniway if Suniway were “interested in attributing the attacks that have been facilitated through their infrastructure,” adding that the said attacker had “administrative rights to servers in their core infrastructure.”

---

10 Ellis-Petersen, Hannah "Maria Ressa: everything you to know about the Rappler editor" *The Guardian* https://www.theguardian.com/world/2019/feb/14/maria-ressa-arrest-everything-you-need-to-know-about-the-rappler-editor 23 July 2019 (Date accessed: 10 April 2020)

11 Centre for Media Freedom and Responsibility, Philippine Centre for Investigative Journalism, National Union of Journalists of the Philippines, Philippine Press Institute "[OPINION]: Speak truth to power, keep power in check" *Rappler* https://www.rappler.com/thought-leaders/201688-speak-truth-power-press-freedom-philippines 03 May 2018 (Date accessed: 10 April 2020)

12 A second look at the charges filed vs. IT companies over news sites cyberattacks https://www.bulatlat.com/2019/04/05/a-second-look-at-the-charges-filed-vs-it-companies-over-news-sites-cyberattacks/

In the complaint, the alternative media outfits under attack identified three causes for legal action for the two tech companies: clear abuse of right, losses and injuries sustained by the plaintiffs, and the violation of the plaintiffs' freedom to maintain publications.

As of February 2020, the IT companies and media outlets have reached an agreement.[13] In a joint statement, IT companies expressed "their utmost respect and full support of press freedom as a constitutional guarantee and a tenet of a democratic society".

"As defendants have no prior knowledge of, much less consented to, the use of IPC's and Suniway's respective cyber-infrastructure for the perpetration of these cyberattacks, defendants commit to support a free press". In the joint statement, IPC and Suniway commit to developing mechanisms that could combat attacks in the future.

The media groups ended up collectively withdrawing the charges before the court and the results were considered a small victory by the group, as they affirmed their right to press freedom and free expression and provided a promise of future vigilance.

Detecting a DDoS Attack

On a user level, the most common way to know if a website is down is to get a 503 error when you try to access it. This means the server is unable to handle requests. But a 503 error doesn't always mean a DDoS attack has occured. They often appear when a site is undergoing routine maintenance, like an upgrade to a new content management system. If this is the case, web maintainers will intentionally send out this error code to let people know the site is currently unavailable.

Usually, digital security practitioners learn about a potential DDoS attack after being contacted by someone whose website was attacked, as an accidental discovery when fixing other issues or due to a notification from a monitoring system informing of high resource consumption (many attacks beyond DDoS manifest through performance problems). These alerts may also arrive from third parties (e.g. a hosting platform), or the website may just go down.

According to Qurium's investigation of the DDoS attack against Bulatlat, the website traffic on January 29, 2019, one of the most successful attacks on the site, was nearly equal to a half a year's worth of requests in a minute.[14]

Can you predict a DDoS attack?

On a technical level, it is not possible to predict a DDoS attack. However, incidents against similar press or human rights organisations may indicate future DDoS attacks against other organizations.

In hindsight, cases of attacks against human rights organisations and media aforementioned, could have served as warnings for future DDoS attacks against smaller alternative media websites, demonstrating the importance of establishing links between different incidents and digital security attacks.

[13] Parties to cyber attack cases reach agreement https://www.bulatlat.com/2020/02/24/parties-to-cyberattack-cases-reach-agreement/

[14] Ibid.

Impact of a DDoS Attack

While an instance of a DDoS attack against a media or human rights organisation is a cause for worry, there are multiple angles to consider.

First, given the context in which these attacks tend to happen, the most lasting impact of DDoS attack may be less about the technical damage and more about the emotional impact of the attack. Upon seeing how their work is actively monitored, the targeted organisation or movement may self-censor in the future, in what's called a "chilling effect".

At the technological level, many human rights and alternative media organisations do not have the same technical capacities and resources that their attackers have. In an instance of a DDoS attack, human rights or alternative media organisations will have to deal with both the immediate technical inconvenience of the attack and the future adaptation required to prevent it from happening again. This could mean:

- Changing web hosts.
- Contacting digital security experts for support.
- Making changes in their behaviours as an organisation.
- Building capacities within the organisation to understand what is happening and to mitigate further attacks.
- Building individual and organisational digital security skills – all of which require resources (human, financial, technical, time).

A DDoS attack against a minimally-staffed, low-resourced organisation's website is not a problem they need on top of the likely many issues they are already confronting.

A DDoS attack, especially one that is sustained for months, may have a disempowering effect on those involved in human rights and alternative media work. This could mean:

- The inability to reach one's audience during a DDoS attack.
- The inability to receive donations, if an organisation is reliant on their website for fundraising.
- The inability to publish critical and timely information to the public, especially challenging in cases where up-to-date news and information about a current event (i.e., elections) is necessary.
- The feeling of "being silenced" and censored.

In the Philippine case, the DDoS attacks against the alternative media websites had the positive effect of garnering support from other journalists and activists. Mainstream media companies in the country also covered the story, which made the attacks against these websites more visible.

The forensic investigation that Qurium conducted provided key evidence that allowed media groups to hold IT companies accountable and show the government that these alternative media sites will not be silenced.

Mitigation strategies and tactics

There is a lot to be learned from the Philippine example.

First, the importance of having trusted and secure web hosting services is critical in mitigating and investigating DDoS attacks. Services like Virtual Road or Greenhost, or web hosting services for human rights and / or independent media organisations are key partners in understanding the why's and how's of DDoS attacks. Without Qurium's forensic investigation on sites like Bulatlat.com, media groups in the Philippines would not have been able to hold those responsible for the DDoS attacks accountable or to use the evidence of DDoS attacks in support of press freedom.

Second, it showed the importance of human rights and independent media organisations being able to prepare their websites for DDoS attacks, especially when publishing information or reports that are critical of those in power.

Though services like Cloudflare also offer DDoS protection, it is worth noting that Bulatlat used Cloudflare when they were attacked in December 2018 and that the service was unable to handle the attacks in January 2019. Cloudflare is a powerful service, but it doesn't promise DDoS protection in 100% of cases.[15] Therefore, there needs to be both proactive and reactive systems in place to minimise damage and keep the content online. Access Now's Digital First Aid Kit (DFAK)[16] and OpenInternet[17] have further recommendations on ways to test and secure web hosts from DDoS attacks.

Third, through partnerships with other organisations and through social media and other news sites, the independent media organisations were able to report the incident as it happened, garnering support from press freedom advocates. This may have mitigated the chilling effect of a sustained DDoS attack against independent media sites. While the DDoS attacks attempted to silence independent media, it ended up having the opposite effect.

Fourth, the media organisations' connections to the digital security community–facilitated by prior partnerships with organisations and individuals–enabled them to respond to the attacks in a timely manner, including the migration of their web host during the attack.

While predicting a DDoS attack is not possible, there are strategies and tactics that human rights and independent media organisations can use to increase their ability to respond to a DDoS attack.

Preparing for an attack

- Have a trusted and secure web-host, ideally with specific DDoS protection such as Cloudflare or Deflect. There are a few community guides with helpful questions to ask before choosing a host:
    - My website is down, what is going on?, Digital First Aid Kit[18]
    - How to assess a vendor's data security[19] by EFF, 2018
    - What to Ask Before Picking a Hosting Provider[20] by Equalite written during a Responsible Data Forum in 2014
- Document and store in a secure location:
    - Who built your website? Would they be available to help in case an attack happens?
    - Was your website built using Wordpress or another popular CMS platform?

15 https://www.wired.com/story/cloudflare-unmetered-mitigation-ddos-attacks/
16 https://digitalfirstaid.org/en/topics/website-not-working/
17 https://github.com/OpenInternet/MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md
18 https://digitalfirstaid.org/en/topics/website-not-working/
19 https://sec.eff.org/blog/how-to-assess-a-vendor-s-data-security
20 https://learn.equalit.ie/wiki/Responsible_Data_Forum_on_Hosting

    - Who is your web hosting provider?[21]
- Be aware of what is happening in your context. Are there official statements against organisations like yours from the government? Are there known threats against organisations like yours? Have similar websites been attacked in the past?
- Plan accordingly when you publish stories, information, reports or news that are critical of the government or those in power.
    - If you plan to launch especially controversial news, make sure you talk to your web hosts and ensure your website is as up-to-date as possible. You may want to back-up the website right before publication, so you can find other ways to share the information if the site goes down.
    - Even if you aren't launching a large campaign or controversial article, it's best practice to back-up the website and all accompanying media files regularly. Talk to your host service about setting up an automatic backup system and saving the site somewhere offline in case the host is inaccessible.
- If you can, connect to trusted digital security practitioners in your location and/or context. The Access Now's Digital Security Helpline[22] is one such resource. Others include:
    - Ukraine: Digital Security Lab Ukraine https://dslua.org
    - Armenia: CyberHUB-Armenia https://cyberhub.am/hy
    - eQPress secure hosting (https://equalit.ie/eqpress) and Deflect DDos protection (https://deflect.ca) for NGOs
- Establish an incident response team within your organisation to address DDoS attacks. Depending on the size of your organisation, the team could be anywhere from one to three people. While the team would support the organisation following various types of physical, digital and legal incidents, the specific needs following a DDoS attack could include:
    - Direct and constant communication with the webhost during the attack, including reporting the site being down to the webhost.
    - Reporting the incident to digital security practitioners.
    - Reporting the incident to the rest of the staff and the board, including developments in the incident.
    - Reporting the incident to your community and / or audience, including developments in the incident.
    - Documenting the incident – from the time of first discovery, status reports from the web host, information the organisation shared of the incident, processes and actions taken to respond to the DDoS attack.

Responding when attacks happen

- The Digital First Aid Kit provides a questionnaire to diagnose other potential problems your website may be experiencing. You can access the questionnaire or the full research.
- Ask the host for web server logs, FTP/SSH connections and admin panel logins. With the logs, you can either analyse in-house (if you have organisational capacity), or share with an experienced security practitioner. Logs are simple text files that note what is happening on a server. If someone accesses it from a certain IP address, you may see that noted in the logs. They are essential for any type of deeper analysis of the attack. If most of the visits logged are from the same IP address or region, it may give you some clues as to who is attacking the site.
- Keep in close communication with your web host about the status of the DDoS attack.

[21] https://digitalfirstaid.org/en/topics/website-not-working/
[22] https://www.accessnow.org/help/

- Message your audience through other channels (social media, private channels) and explain why your site is down.
- Reach out to digital security practitioners, and report to them what has happened. They may be able to provide extra support for your organisation and/or your webhost. Be prepared to answer questions from the practitioner about the attack[23], such as:
    - What is going on, exactly? Errors, timeouts or slowing down?
    - What were you doing at the time of the website crash?
    - Is part of the website affected or the entire site?
    - Have you changed anything on your site recently?
- Share information about the incident as soon as you confirm what kind of attack it is.
- Keep updating your community and audience as you find out more from your web host and anyone supporting your organization's digital security.
- If you have set up a back-up site, activate it and let your audience know where they can access your new site.

Zoom-in: Questions for practitioners to ask when investigating compromised websites

As Internews reports[24], there are several important questions to ask at the outset of any investigation. For example, questions about the specific times incidents occurred will be important when analyzing logs further down the line. Other key questions include:

- What is happening exactly? Errors, timeouts, slow loading times? Can you send a screenshot?
- What were you doing when the incident occurred? Do you have any idea what might be triggering the problem?
- Is the entire website affected or just a part of it?
- How long has it been happening? How often does it happen? When did it happen last?
- If it's a recurring problem, does it need to be fixed by someone each time? What actions have they taken?
- Have you changed anything on the website recently (e.g. plugins)? Who would know if something has been changed?
- Is there another website administrator who wouldn't want me exploring the system?
- What steps do you approve for me to take? Can I install things on your system?
- Is there a specific time slot I should work on your system during (e.g. weekends, night time)?

After the attack

- Talk to your web host to collect more information about the attacks to share with organisational security practitioners. Discuss what they can do to mitigate further incidents and see if they can do forensic investigation on the attack.
- Consider whether there are other vulnerabilities on the website that may have led to the DDoS attack, such as open web forms without CAPTCHA or old admin credentials using default passwords.

[23] Help, my website's been hacked! Triage and collecting Indicators of Compromise" https://globaltech.internews.org/blog/help-website-hacked
[24] Ibid

- Revisit the technical documentation of the incident, including logs and analysis from your webhost, the information your organisation has sent out about the incident, and the organisational processes that were triggered during the incident to understand what worked and what could be improved.
- Debrief on the incident with the team to try to understand the root cause of the attack, how the staff is responding to it and to strategize ways forward post-incident.

In summary, the most critical aspects that prevent and mitigate DDoS attacks are:

- Regular updates and careful management of content management systems, like Wordpress
- Trusted technical support from web hosters and security practitioners
- A community of peer organisations who can share news about the attacks and help garner support
- A culture of learning and reflection within the organisation to implement new, stronger systems following an attack

Because of the connectedness of the independent news outlets in the Philippines to networks of technical and emotional support, they were able to come out of the attacks stronger and more aware of the risks they face.

Resources

- "What is a DSoS Attack?" Cloudflare https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Date Accessed: 06 April 2020)
- An Ambitious Plan to Stop DDoS for Good Has Its Limits https://www.wired.com/story/cloudflare-unmetered-mitigation-ddos-attacks/
- Website not working https://digitalfirstaid.org/en/topics/website-not-working/
- What to do when your website goes down https://github.com/OpenInternet/MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md
- What to do when your website goes down: Before you choos https://github.com/OpenInternet/MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md#before-you-choose
- How to assess vendor's data security https://sec.eff.org/blog/how-to-assess-a-vendor-s-data-security
- Responsible Data Forum on Hosting https://learn.equalit.ie/wiki/Responsible_Data_Forum_on_Hosting
- Help, my website's been hacked! Triage and collecting Indicators of Compromise" https://globaltech.internews.org/blog/help-website-hacked