Analysing attacks: A guide to building archetypes and case studies

June 2020

THE ENGINE ROOM

Internews

Contents

Introduction

This guide looks to support organisational security practitioners from all backgrounds to analyse digital security attacks collected through incident reports and other sources–such as media, community sources and threat research–in order to help a broader community of practitioners and human rights organisations identify trends of attacks and learn about mitigation strategies.

This guide provides two tools: attack archetypes and case studies.

Attack archetypes illustrate threat patterns and scenarios that are commonly seen. They can help human rights organisations identify recommended digital protection practices, based on their organisation's profile and the type of attacks they are experiencing (or might one day experience due to their profile).

Case studies seek to support practitioners and civil society organisations by illustrating the consequences of attacks and the benefits of deploying mitigation tactics, through a detailed description of a real-world scenario.

Building an attack archetype

Collecting information

In order to identify typical threat patterns, it's important to collect the following basic information **describing the attacks**:

- Date of the attack (month and year, at the least).
- The target's profile (individuals or organisations), including information of their goals, size, the type of work they do (journalists, activists, human rights defenders, campaigners, lawyers, for example) and what sector they are working in (anti-corruption, transparency, accountability, women's rights, LGBTQI+ rights, land rights, for example).
- Location of who were attacked (region or country, at the least). The detail level will depend on sensitivity and where this will be shared.
- Description of the attack. The detail level will depend on sensitivity and where this will be shared.
- Type of attack, including: Account takeover, DDoS, Malware, Phishing, Spear-phishing, Physical attack, Policy-related threats, Watering hole, Website hacking or Website blocking due to censorship.
- Information on how the incident was detected.

Additional relevant information regarding **the targeted groups** includes:

- What signs indicated the individual or organisation that they were attacked?
- Are there signs that indicate the group was targeted with this attack? For spear-phishing attacks, for example, what exactly made the target individual/organisation aware or suspicious that it was a spear-phishing?
- Is there documentation or understanding that the group has been targeted in the past?
- More specifically about their background, what kind of work are they doing? If it's an activist group, which issues do they work on? If it's a journalist, what topics do they cover?

Additional relevant information regarding **the context** of the attacks:

- Political, economic or major social events happening in the country/city/location during the attack. For example, elections or new policies being implemented at the time.
- Consider if the attack happened during a critical time in the country or region, such as anniversaries of social revolts, protests or major actions led by civil society groups (such as legal actions).
- Were there similar incidents in the communities or groups the human rights defender, activist or journalist is involved in? Were there other incidents, even if they seem unrelated, happening in the same period?

Analysing the data

After you've collected incident information, you may be able to identify trends in how attacks unfold–patterns regarding a target organisation, group or individuals. To draw these trends out, you can start by reviewing organisations that are working in similar contexts and sectors, or that share other elements in common, and then reviewing the attacks they experience. Or, you can start by reviewing attacks and their goals. For example, is the attack or are the attacks intended to interrupt the publication of certain investigations? Or to intercept communications? Or access relevant information that the organisation holds?

Another way practitioners can help with analysing information, is by adding tags to the information collected, so they can later filter and search through documents, threats, logs and incidents.

In order to build out these trends, identify the shape of the attack archetype, and share the archetypes we suggest following the next structure:

Template for attack archetypes

A. Introduction with context information for the development of the attack archetype.
B. Types of attack.
C. Description of targeted individuals or organizations.
D. Contextual information from the time of the attacks, including relevant political, economic or major social events. For example, during national-level elections or organised protest.
E. Community contextual information, if relevant. For example, an attack may be conducted at the time when other members of the community are being targeted through similar attacks or threats. These attacks may be similar or different than the one described in the archetype.
F. Organizational contextual information, if relevant. For example, attacks may happen during staff transition or turnover.
G. Typical process of how the attack unfolded within the organisation or against an individual, including how the attack can be detected, what steps the individual or organisation can take afterwards, and when the organisational security practitioner begins their support. Along with these, it can be useful to include if the organisation's community response was relevant to mitigate the effects of the attacks.

A non-comprehensive archetype example

Introduction

The purpose of this archetype is to illustrate a typical threat pattern and scenario, describing the organization's profile and types of attack they are experiencing, in order to help human rights organisations identify recommended digital protection practices.

This archetype will focus on attacks looking to interrupt an organisation's or media publishing of relevant information online, with a focus on DDoS attacks.

Types of attack

A DDoS attack remains one of the most effective ways of forcing a website to shut down. “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] 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.

Other attacks with the goal of interrupting an organisation’s or media publishing of relevant information online may include:

- Account takeovers, spear-phishing attacks or physical attacks involving devices, with the aim of accessing to websites administration in order to delete or modify information.
- Website pages defacement.
- Redirecting site to other content, such as scam or malware websites.
- Brute-force attacks.
- Online harassment on social media, by reporting content to platforms that is consequently taken down by the services.
- Censorship attempts to block websites or social media accounts.

Description of targeted individuals or organizations

- Independent media organisations
- Independent media consortiums
- Human rights organisations expressing dissent from current Government or authorities

Relevant social, political and economical context

Many cases indicate that attacks happen on or around significant dates, including anniversaries of events associated with social unrest and dates that hold special relevance to government opposition movements. Regarding media organisations, attacks often coincide with the publication of reports or stories with a critical perspective.

Relevant community context

Reports on attacks or threats looking to silence organisations or media show that other members of the community may be targeted too. Attacks may happen digitally and/or physically, including online harassment, death threats, intimidation, website attacks, revoked registration or denied franchise renewal, verbal abuse, and police surveillance.

Relevant organizational context

There is no sufficient information.

Typical process of how the attack unfolded within the organisation or against an individual

The method of detection of these attacks varies. In the case of a DDoS attack, digital security practitioners typically learn about a potential attack after being contacted by someone whose website was attacked, as an accidental discovery when fixing other issues or due to a notification

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

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.

Steps to be taken afterwards also vary, but according to an Attacks Trends Report published by The Engine Room from 2020, these may include:

For DDoS attacks:

- Re-setting Cloudflare configuration[2] by:
  - Locking down IP of Cloudflare to hosting VPS server.
  - Blocking source of attack via geolocalization[3].
  - Enabling Rate Limiter[4].
- Migrating the website from Cloudflare to Deflect[5].
- Following a mitigation process led by Deflect.
- Providing technical consulting for future litigation.
- Changing to a different hosting plan (due to an attack that increased the traffic above the organisation's hosting budget).

For attacks related to accounts takeovers:

- Recovering the lost account, with help of practitioners from Access Now' Digital Security Helpline.
- Assessing and strengthening user account settings, such as 2-factor or multifactor authentication.
- Conducting training on account security and digital security, as developing an emergency plan in case attacks continue for a longer term mitigation strategy.

Creating attacks consequences case studies

Collecting information

For creating this tool, basic information to collect **describing the attack** includes:

- Date of the attack (month and year, at the least).
- The target's profile (individuals or organisations), including information of their goals, size, the type of work they do (journalists, activists, human rights defenders, campaigners, lawyers, for example) and what sector they are working in (anti-corruption, transparency, accountability, women's rights, LGBTQI+ rights, land rights, for example).
- Location of who were attacked (region or country, at the least). The detail level will depend on sensitivity and where this will be shared.

[2] https://support.cloudflare.com/hc/en-us/articles/200170196-Responding-to-DDoS-attacks
[3] https://support.cloudflare.com/hc/en-us/articles/217074967
[4] https://www.cloudflare.com/rate-limiting/
[5] https://deflect.ca/

- Description of the attack. The detail level will depend on sensitivity and where this will be shared.
- Type of attack, including: Account takeover, DDoS, Malware, Phishing, Spear-phishing, Physical attack, Policy-related threats, Watering hole, Website hacking or Website blocking due to censorship.
- Information on how the incident was detected.

Additional relevant information regarding **the response to the attack** include:

- Whether the attempt was successful or not.
- Strategies used to respond to attacks and mitigation techniques, including both immediate actions and preventive measures to protect for future attacks, and details on any further forensics that took place.
- Information related to collaboration with other practitioners, communities, companies or organisations to detect or develop mitigation next steps.
- Whether reports or alerts were produced or and how indicators were shared (for example, in Slack or Mattermost groups, private sector contact, Signal group, MISP[6] or others).

Additional relevant information regarding **the impact of the attack** include:

- Information on social, political or legal outcomes following the attack.
- Information related to the impact of the incident on the individual(s) and the organisation:
    a. If they did report the incident, did they seem stressed out, afraid or concerned?
    b. If the incident was resolved, how was the individual or organisation able to recover from it?
    c. Did they take steps to prevent the same attack from happening again? If so, what were they?
    d. What were the consequences of the attack on the target individual? Look to respond to this question holistically. A digital attack may affect a person on a physical level resulting in a change of residence or an entire organisation on a psychosocial level resulting in professional psychosocial support for all staff.The attack could lead to legal escalation on behalf of the organisation.

Template for attacks consequences case studies

Using the information collected above, a case study following the story of a particular organisation, group or individual can be fleshed out using the following structure:

A. Introduction with context information for the development of the case study.
B. Type of attack.
C. Description of the example attack.
D. Information on how the attack was detected.

[6] https://www.misp-project.org/

E. Impact of the attack.
F. Mitigation strategies and techniques.
G. Resources to complement mitigation strategies and techniques.

How to safely share these tools with the community

1. If you are collecting information specifically to build any of these tools, share information with the targeted group beforehand around what you plan to do with the information and how you will be sharing their story with others.
2. In some cases, practitioners report with code names, differentiating them in order to better detail their analysis.
3. Do context research that allows you to de-identify a group or an individual if the case you are working with is not public. For example, if there is only one Black Lives Matter (BLM) chapter in a given city, for example, then referring to the city and a BLM group could make identifying the person very easy.
4. If the information you are collecting is not public, make sure you get consent with the targeted groups before sharing the information with other practitioners or with a large network.
5. Read through the information and check for any names, contact information, or other identifiable details that if shared with the wrong person could result in harm to the targeted group. Pseudonyms don't always protect your sources.
6. Only share with trusted groups, and when you share, specify the guidelines for further sharing.
7. Know that if you write down identifying details and/or share detailed information with others, it's possible it could end up in the wrong hands. Sacrifice detail to protect targets of the attack and take extra precautions when necessary.
8. If you find yourself needing to omit large sections of the case study for the safety of the target, it may make sense to turn it into an archetype, which requires significantly less detailed information to be useful.