Attacks trends report

June 2020

THE ENGINE ROOM

Introduction

This trends report was developed based on incidents reported by organisational security practitioners from Eastern Europe, the MENA region and Southeast Asia, as reported in cases provided by Internews and by Access Now's Digital Security Helpline[1].

Incidents were mostly collected through incident trackers, which are a documentation tool used by practitioners to document digital security incidents experienced by human rights organisations, media, activists and journalists, either reported to practitioners or publicly shared through other means. The report is based on anonymous or aggregated information. These incidents account for attacks received, including successful and unsuccessful ones.

Based on the incident reports we reviewed **there were 149 cases between April 2019 and March 2020.**

This number is not comprehensive of the total attacks on civil society organisations, journalists and activists, as it only represents cases reported by a subset of practitioners based in Eastern Europe, the MENA region and Southeast Asia.

During the period looked at, the most common types of attacks were:

- Account takeovers
- Phishing and spear-phishing attacks
- Website hacking attacks
- DDoS attacks
- Malware-related incidents

a) Account takeovers

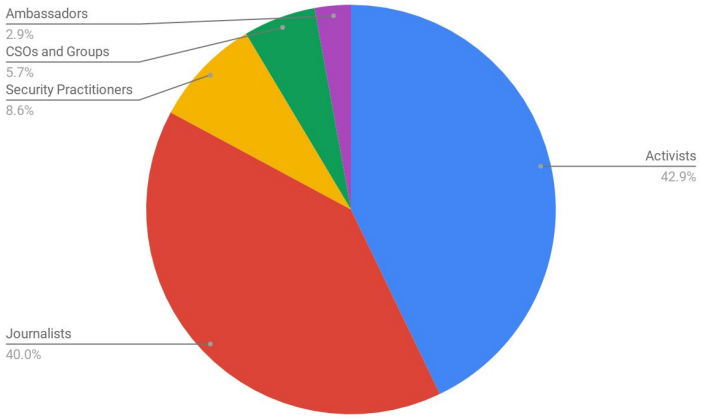
There were **80 cases of account takeover attacks reported in the period analysed**.

From the information collected, at least 20% of them were conducted between January and March 2020.

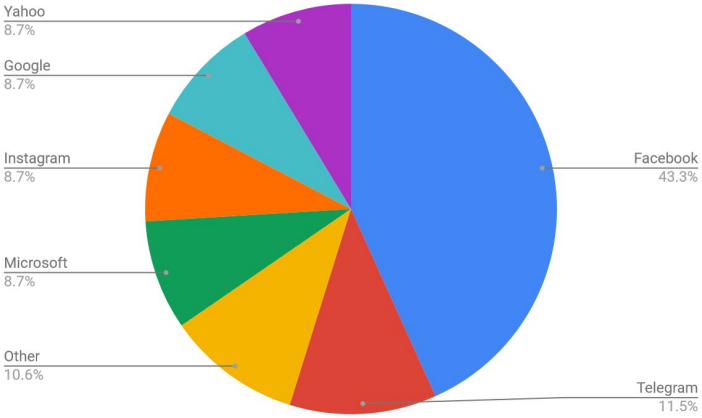
Of the 80 account attacks reported, among the ones with further details about targets (35 cases), incidents were directed mostly to activists (15 cases), followed closely by journalists (14 cases). Besides these, three civil society organisations staff and one Ambassador were targeted.

[1] https://www.accessnow.org/help/

In addition to the target individuals described above, there were three reported attacks against organisational security practitioners.



Of the 80 account attacks reported, among the ones with further details around platforms (34 cases), attacks looked to take over Facebook accounts (42% of the documented incidents), followed by Telegram accounts (12% of cases) and Microsoft, Instagram, Google and Yahoo accounts (each accounting 9% of cases). Other platforms targeted include other email services, Facebook pages, Apple (through AppleID) and Airbnb.



Reports indicate that in some cases, users became aware of the attack due to receiving a password recovery message.

Some of the mechanisms included spear-phishing attacks and device-seizing after detentions.

Mitigations

Strategies used to respond to attacks included:

- Reaching out to the platform for support against attempted takeover or to temporarily suspend the account.
- 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.

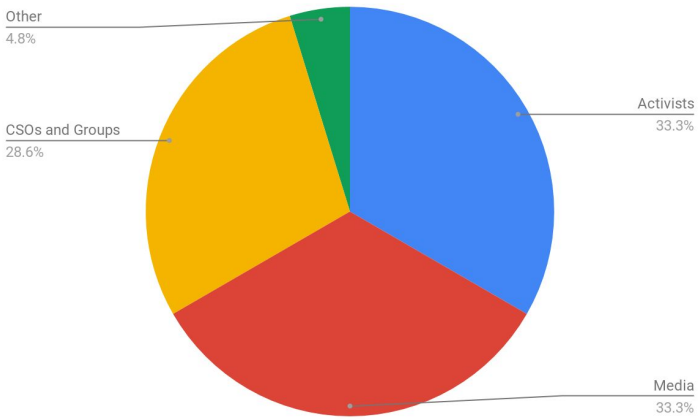
In cases where the compromised device was seized by authorities, strategies included:

- Reaching out to the platform to temporarily suspend the account.
- If an activist had been detained, waiting for them to be released before conducting next steps.
- Preventively revising the device or guide defenders in doing so, to make sure these are sanitized before supporting practitioners regain access to their accounts. This is particularly critical in contexts where authorities force activists to give them access to social media accounts,–regardless of the legality in a given context.
- Replacing the seized device with a new one, if possible.
- Reaching out to organisations specializing in device forensics analysis if needed.

b) Phishing and spear-phishing attacks

There were **27 cases of phishing and spear-phishing attacks documented** during the period, including one spear-phishing attack directed to eleven accounts.

Of the 27 cases reported, among the ones with further details around targets (21 cases), incidents were directed mostly to individual activists (7 cases) and to journalists or media organisations (7 cases) and civil society or human rights organisations, and activists groups (5 cases).



Based on incidents that reported times of the attacks (18 cases), attacks were 2.5 times higher between January and March 2020, than it was between July and September 2019. They occurred across a varied set of platforms, with Facebook messages being used most commonly. Other platforms where messages were sent include emails (including organisational e-mails), Twitter and SMS messages.

Some of the mechanisms included:

- Emails with tampered email addresses (allegedly sent from the individual's own email).
- Emails mimicking legitimate online services.
- Messages including links mimicking URLs of trusted media outlets where by clicking, you are asked to input your social media credentials.
- Messages and URLs mimicking Google Calendar event invitations.
- Ransom demands.
- Polls through private Facebook messages.
- Message supposably including a nude video to lure a user into clicking.

Mitigations

Strategies used to respond to attacks included:

- Reporting attacks to social media platforms, including URLs' domains and their IP addresses.
- Support in securing e-mail and social media accounts, such as implementing 2-factor or multifactor authentication for accounts.
- Providing guidance on identifying phishing attacks.

c) Website hacking

There were **17 cases of website hacking documented during the period**. Of the cases reported, among the ones with further details around targets (10 cases), incidents were directed mostly to media organisations (7 cases), followed by civil society or human rights organisations and activists groups (4 cases).

In terms of the mechanisms of the attacks, these included:

- Attempts to log-in to the Wordpress admin panel.
- Website page defacement.
- Site redirecting to scam or malware websites.
- Brute-force attacks.

Mitigations

Strategies used to respond to attacks included:

- Reporting the issue to the website host.
- Reaching out to website managers.
- Setting the website in maintenance mode.
- Recovering the website through a previous back-up, if possible.
- Researching the attack[2] for malware by:
    - Comparing files with website backup files.
    - Reviewing web server logs.
- Cleaning up websites from malicious code.
- Strengthening the platform's security by:
    - Installing web applications firewalls.
    - Removing outdated or unused Wordpress plugins.
    - Tightening Wordpress security plug-ins.
    - Enabling logging and alerts for website attacks.
    - Updating Wordpress and installed plugins regularly.
    - Implement a threat detection and monitoring application.
- Migrating from a Drupal to a Wordpress platform.
- Backing up the website.
- Referrals to Cloudflare's Project Galileo[3] for DDoS protection.

[2] https://globaltech.internews.org/blog/help-website-hacked
[3] https://www.cloudflare.com/galileo/

d) DDoS attacks

There were **11 reported cases of DDoS attacks**, four of them directed at media organisations and one at a human rights organisation.

Strategies used to respond to attacks included:

- Re-setting Cloudflare configuration[4] by:
    - Locking down IP of Cloudflare to hosting VPS server.
    - Blocking source of attack via geolocalization[5].
    - Enabling Rate Limiter[6].
- Migrating the website from Cloudflare to Deflect[7].
- 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).

Other attacks

During the period, there were **four cases of malware incidents reported**, which do not show possible trends to consider. Each of them was targeted to a different actor group: a human rights organisation, a journalist, an activist and a group of journalists and human rights organisations. This last one remains as a threat, as no incidents were reported in the analysed period. Suggested mitigation strategies can be found in the documentation of the webinar from the Threat Analysis and Sharing series facilitated by Nataliia Onyshchenko, ICT Coordinator for Internews Europe[8].

Other attacks include physical attacks involving devices, personally identifiable information supposedly leaked, spoofing, censorship attempts to block websites or social media accounts and credit card fraud where donations were made using a stolen credit card.

[4] https://support.cloudflare.com/hc/en-us/articles/200170196-Responding-to-DDoS-attacks
[5] https://support.cloudflare.com/hc/en-us/articles/217074967
[6] https://www.cloudflare.com/rate-limiting/
[7] https://deflect.ca/
[8] https://globaltech.internews.org/blog/help-website-hacked