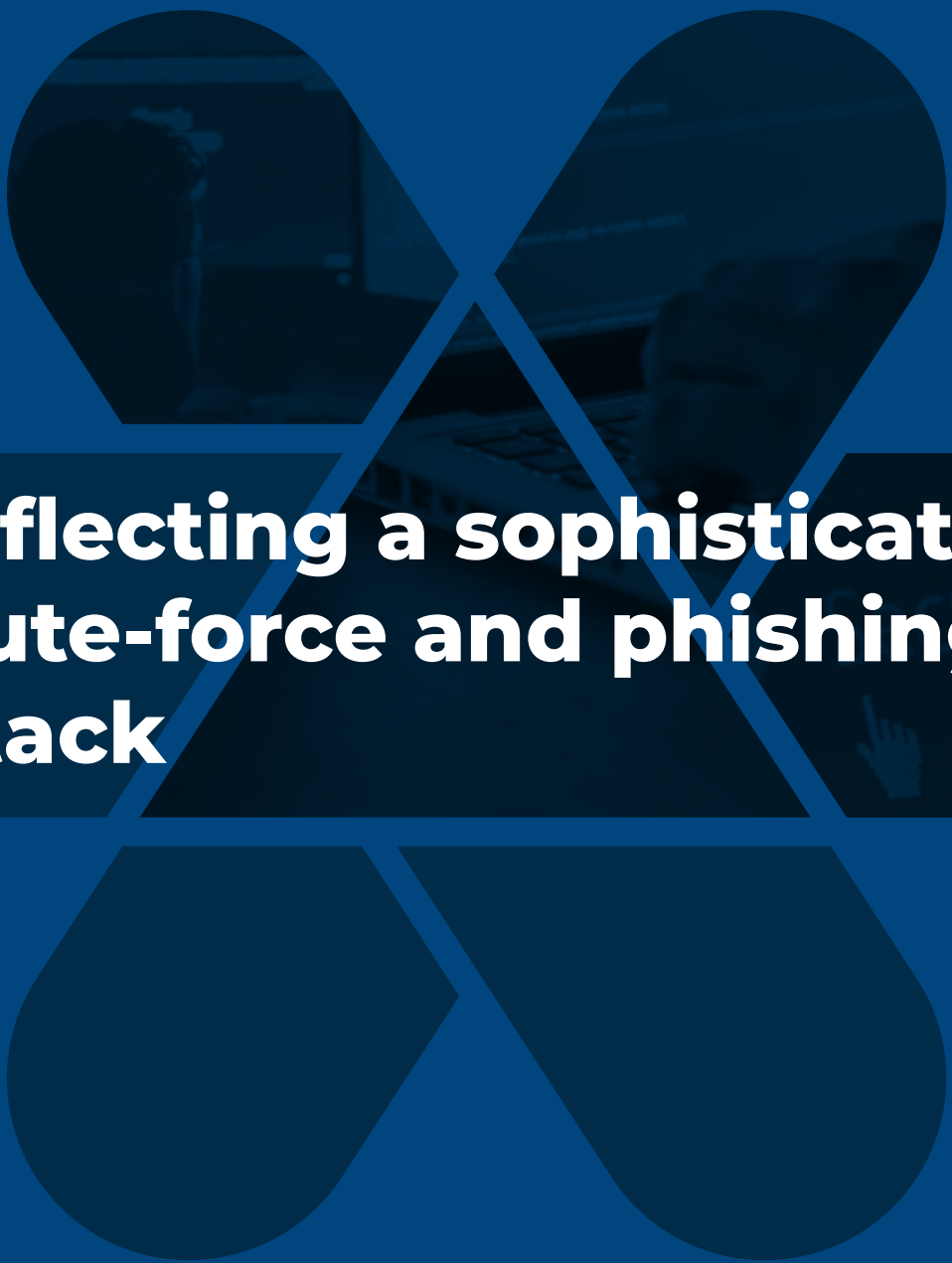
Solidarity Playbook



Deflecting a sophisticated brute-force and phishing attack

International Civil Society Centre

CyberPeace Institute

solidarityaction.network

1. Overview

The organisation in this case is a medium-sized civil society organisation working in the humanitarian sector. It has a global focus with presence on all continents. Its headquarters is in Europe, and it has offices in approximately 20 countries.

In 2021, the organisation was targeted by a brute-force attack through their webmail, followed by targeted phishing emails on the same day. With support from an external cybersecurity company and in cooperation with the organisation's management and staff, the IT team managed to avert the intense attack that lasted for approximately one full working day. It took several weeks to manage the aftermath of the attack.

2. What happened?

In the summer of 2021, the organisation was targeted by a brute-force attack. By 9:30 am on the day of the attack, the Chief Information Officer (CIO) and the IT team **noticed a high volume of login attempts through the organisation's webmail**. The attackers had managed to collect correct email addresses of the organisation's staff. Organisational emails typically contain employee names in a particular format; thus, the attackers probably used LinkedIn to identify employees, then figured out the format the organisation used for staff email addresses. The attackers then bombarded the system with login requests for the email addresses they had identified, likely using passwords randomly generated by a bot.

BRUTE-FORCE ATTACK

A cyberattack using a trial-and-error approach to guess possible combinations and decode login information to gain unauthorised access to a system. Organisations should make sure their staff use strong passwords to buy themselves time to respond to this type of attack.

TechTarget (n.d.): ***Definition: Brute-force attack***

The attackers were unable to access the system through the brute-force attack, but this was likely not their only goal. The number of login attempts within the first two to three hours of the attack put an **unusual amount of pressure on the system, representing a denial-of-service (DoS) attack**. As a standard security precaution, if a certain number of incorrect login attempts was made for a staff member's account in a given time period, the user would be blocked. **Many staff members were locked out of their accounts and sending requests to the IT team** to regain access to their accounts. The attack therefore put pressure on the organisation's IT team and systems, and it caused the system to lock out genuine staff members and prevent them from doing their work.

DENIAL-OF-SERVICE (DOS)

DoS is an attack technique in which a network, service, or server is flooded with excessive traffic to cause it to cease functioning normally.

CyberPeace Institute (2022): ***Glossary of cyber terms***

A few hours after the brute-force attack began, the attackers sent a phishing email to almost everyone in the organisation. The email was well written and looked like it was coming from a staff member on the IT team. The email requested that, due to the ongoing brute-force attack, staff log in using the following link. **The link contained in the phishing email led to a fake webmail landing page that looked very similar to the organisation's webmail page, except for one character that was intentionally omitted** (an example of '*domain spoofing*'). On the fake webmail landing page, staff were prompted to enter their login information and password, which would likely lead to malware being installed.

PHISHING ATTACK

A phishing attack is a common cyber threat that consists of a fraudulent communication posing as a reputable source. It aims to trick the recipient into providing sensitive data or installing malware. Phishing attacks are not only increasing in number but posing more sophisticated threats. For example, **spear phishing** is a targeted phishing attack that exploits real information about the victim to make the source of the attack seem credible.

Solidarity Action Network (2022): ***Navigating cybersecurity: Guidance for (I)CSO professionals***

DOMAIN SPOOFING

A fake website name or email domain created to trick the user into sharing personal information (such as login credentials or credit card details) or downloading malware.

Solidarity Action Network (2022): ***Navigating cybersecurity: Guidance for (I)CSO professionals***

Fortunately for the organisation, the IT colleague whose email was used for the phishing attack was on parental leave. The person had been out of office for quite some time and some staff members were aware of their absence, so the phishing email originating from their address raised red flags. Staff forwarded the email to IT, saying that they knew the colleague was out of the office and that the email looked suspicious.

Even after the phishing email had been sent, the attackers continued with the brute-force attack, attempting to log in to different accounts. Ultimately, the IT team decided to take down the organisation's system, temporarily disconnecting it from the internet to prevent further attacks. When they reconnected hours later, the attacks did not continue.

3. Response

The IT team identified the brute-force attack within the first hour of the incident and reached out to a cybersecurity support company they usually work with. Unfortunately, the company was unavailable at the time, so they reached out to another company they had previously worked with on IT infrastructure projects, which also happened to run a cybersecurity support unit. The second company had availability and started moving toward the organisation's premises soon after the call.

To counter the attack, the IT team focused on identifying and blocking the IP addresses from which the attempts originated. Each time the IT team blocked an IP address, the attackers created a new one. According to the CIO, *"It was like a game of cat and mouse."* This process continued for two hours before the attackers sent out the phishing email.

The support team from the cybersecurity company arrived at the organisation's offices shortly before the phishing email was received by employees. **Together, the IT team and cybersecurity company carried out a quick assessment of the situation and determined that the appropriate action was to shut down the internet connection for all the organisation's digital services**. They contemplated shutting down only the webmail services but decided not to, as they recognised that this was a professional attack and all services needed to be checked. Approval to shut down the organisation's IT services was requested and received from the Chief Operating Officer.

The IT team and cybersecurity company began a close review of the incident to ascertain what had happened and determine the actions they needed to take. **They began to secure the organisation's data and resources**. The first step was to identify all staff email accounts that had received the phishing email and delete the email from their mailboxes to prevent staff members from clicking on the phishing link after the systems came back online. The team then scrutinised each account for successful and failed connections, suspicious connections, and unauthorised services. They methodically confirmed that all successful logins were legitimate and that accounts only had access to the organisation's IT services as intended. They also checked to ensure that no new users had been created by someone other than the organisation's IT admin. In addition, they audited all machines in the organisation to make sure that they were updated and ran full anti-virus scans.

After ensuring that there were no vulnerabilities in the organisation's systems, the IT team and external cybersecurity firm created a test environment with an isolated computer (which was not connected to a network) and a 'dummy account' to examine the fake webmail link. They followed the instructions in the phishing email to see what would happen. As suspected, when they entered the login and password on the fake webmail link, malware was installed on the computer. Using standard websites that are freely available, such as www.virustotal.com, they identified the name of the malware used.

While the organisation's systems were offline for a few hours, communication beyond face-to-face interactions in the office was difficult. Given the urgency of the shutdown, the organisation did not have time to put an alternative communication method in place. During this period, the IT team used secure messaging via phone to keep management informed.

After two to three hours, the IT team restored the connection between their services and the internet, notified staff that the system was back online, and asked people to come forward if they had clicked the phishing link. They found that fewer than ten people in an organisation of hundreds had clicked the link in the phishing email, and the computers of these staff members were thoroughly scanned to look for the specific malware. The malware was found on a couple of computers, but they were able to delete it and the computers were not compromised.

When the systems came back online, the brute-force attack had ceased. **The IT team suspects that cutting the connection was a clear signal to the attackers that they understood the attack**. Not long after, the fake webmail site was also taken down. It was unclear to the organisation whether the attackers had stopped completely or changed their approach. In the aftermath of the attack, the organisation asked two other suppliers to help them conduct a post-mortem investigation of the incident. Unfortunately, they did not find out who was behind the attack.

Throughout their response, the IT team communicated what was happening and shared updates with the communications team that were then posted on the organisation's internal website. During the early stage of the brute-force attack, the CIO sent out an email to inform everyone in the organisation about the brute-force attack and ask staff to be prepared for challenges with logging into their accounts. When the IT team were alerted to the phishing attack, they sent a second email to inform staff and ask them not to take any action if they received the phishing email. They further informed staff of the seriousness of the attack and gave them half an hour's notice that they would be disconnecting all of the organisation's services from the internet to address the cyberattack. After the system came back online, the IT team communicated this update to staff. That evening, the team sent out a formal communication to all staff explaining what had happened and how they had responded. In the days following the cyberattack, the IT team regularly updated staff on measures taken to help prevent another brute-force attack – such as patching, temporarily taking services offline, and introducing two-factor authentication – and explained the rationale for each measure taken.

4. Outcome & impact

The outcome of the attack could have been far more devastating if the attackers had not sent the phishing email from the account of a staff member who was on long-term leave. Given how convincingly the phishing email was crafted, if the attackers had used a different account, the IT team might have been alerted less quickly, and more staff members might have clicked on the phishing link and entered their account information on the fake webmail page.

Although the team felt fortunate that the incident was resolved quickly, it was still a stressful time. The CIO had started in the role only a few days before, so while trying to minimise the potential damage of the cyberattack, they were also concerned about how such a disruptive attack might reflect negatively on the IT team. However, management were supportive and there was no criticism of the IT team from management or staff.

Taking the organisation's systems offline disrupted the ordinary work of their staff, but the disruption was only for a few hours. If the IT team and external cybersecurity experts had not made the call to disconnect the systems, the brute-force attack might have continued, which would have been more disruptive in the longer term.

The impact of the attack was contained within the organisation; the organisation does not work directly with local communities, nor do they use third-party services they might have needed to coordinate with. However, they do work with partner organisations. Soon after the initial incident, there was another phishing campaign directed to external collaborators. The phishing email used the names of staff at the organisation, but the email originated from unrelated email addresses, such as "xyz@unknowndomain.com." The external partners alerted the organisation to the attack, but there was little they could do, as the phishing attack originated outside their systems. The IT team informed colleagues internally about the phishing campaign, in case external partners contacted them about it.

The incident impacted how the entire organisation viewed cybersecurity. It was ultimately a learning moment and wake-up call, helping to increase staff awareness that **anyone could be a target** and **cybersecurity starts with each individual**. After the cyberattack, staff began taking security messages from IT more seriously.

After the incident, the IT team **set up a form of two-factor authentication (2FA) as a requirement for webmail**, which was rolled out over the next few weeks.

TWO-FACTOR AUTHENTICATION (2FA) AND MULTI-FACTOR AUTHENTICATION (MFA)

MFA is a layered approach to securing data and applications, in which the system requires a user to prove their identity using a combination of two or more methods each time they access the system. In this way, 2FA – which requires two 'factors' or credentials – is a type of MFA.

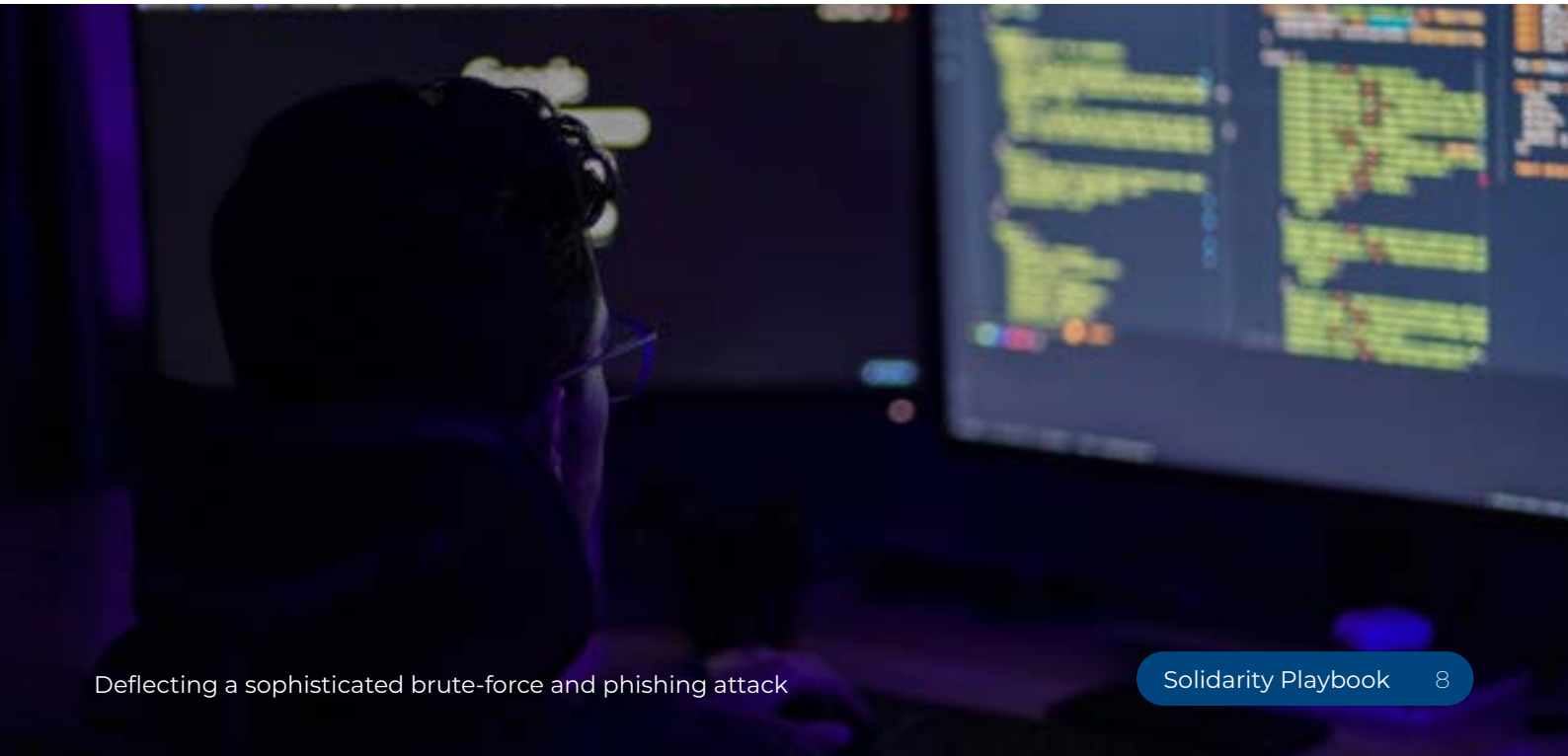
Three main types of credentials or factors are used in authentication:

1. **Knowledge**: authentication using something the user knows, such as a password, pin, or answers to security questions
2. **Possession**: authentication using something the user has, like clicking a confirmation pop-up on a smartphone, receiving a one-time password on a phone, typing a unique code generated by a USB drive, or inserting a smartcard
3. **Inherence**: authentication using something a user is, such as their fingerprint, a scan of their iris, voice recognition, or facial recognition

By using multiple factors to authenticate a user's identity, MFA builds a layered defence and increases security. If one of the credentials is compromised, an attacker must overcome additional barriers to gain access to the account.

*Cyvatar (2022): **What is multi-factor authentication and how to enable MFA?***

Changes aligned with the post-mortem recommendations following the incident have been implemented slowly but surely by the organisation's IT team. These measures include patching the system, ensuring all servers are up to date, and reinforcing monitoring of IT systems. There were existing plans in place to increase the budget and size of the IT team as part of an earlier strategy. The cyberattack contributed to a greater understanding of why these increases were needed and gave additional impetus to make the changes quickly.



Deflecting a sophisticated brute-force and phishing attack

5. Organisational learnings

CHALLENGES

Prioritising internal communication during a crisis

In the midst of responding to a cyberattack, communication may be the last thing on the minds of the responders. For IT staff, setting time aside to email people and communicate about the incident may feel like an ineffective use of time; however, it is important to keep staff informed so they can stay alert.

Finding the balance in what information to communicate

At first, it was unclear where the brute-force attack was originating from and whether there was an internal breach. This lack of clarity created uncertainty about how much information to share. On the one hand, the IT team wanted to keep colleagues informed and reassure them. On the other hand, they did not want to give away too much information, particularly information which could compromise the success of their defence against the cyberattack if there was an internal leak. It was challenging to know what level of information to share and ensure that sharing information didn't constitute another source of vulnerability. How do you share enough to keep people informed while not compromising safety?

Having a small IT team

The small IT team with just a few staff members in an organisation of hundreds of people quickly felt under pressure faced with an attack of this scale. While this was a challenge, it also meant that the IT team rapidly sought external support to deal with the incident.

Uncertainty of the attackers' intentions

In the aftermath of the incident, the organisation sought to better understand the attack and who was behind it. While they did not learn much, what became clear from the post-mortem analysis was that the attackers had means and were determined and serious. An unanswered question for the organisation remains to this day: Did they uncover the whole attack, or is there a chance that the visible attack was only a distraction for something else?

LESSONS LEARNED

System maintenance is important

The need for constant maintenance of systems cannot be overemphasized. After the incident, the IT team noticed that an email server update had been available for a while but had not been installed. It was this vulnerability that allowed the attackers to send the phishing campaign on behalf of an internal user.

A strong budget enables better security

There are tools and resources that can help an organisation monitor the web and detect in advance that a domain spoofing website is being developed for a potential attack. Such tools and resources are helpful preventative measures but require financial means.

Communicating early and regularly is key

The IT team kept the management team updated and the staff informed throughout the attack, sharing sufficient information on a need-to-know-basis. This communication helped address any discomfort that people might have felt at different stages of the incident and was reassuring.

Don’t panic, anyone can be a target

Cyberattacks can cause stress, panic, and regret. In the moment, it was beneficial for the IT team to limit outward expressions of panic or obsession about what could have been done differently to allow the organisation to focus on the issue at hand. The team noted that staying calm was an important part of being able to assess the situation holistically, determine what kind of help they needed, and ask for that help. There were a lot of potential solutions to this incident, so staying calm and patient helped the team to plan and take things one step at a time.

Discover more case studies
solidarityaction.network/cybersecurity

Solidarity Playbook

Deflecting a sophisticated brute-force and phishing attack

Sacha Robehmed and Nonso Jideofor

March 2023

International Civil Society Centre

CyberPeace Institute

In partnership with