Case study: Spear-phishing attacks

June 2020

THE ENGINE ROOM

Internews

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.

What is spear-phishing?

Phishing is an attempt to trick the user into giving up passwords or login credentials - among other personal or sensitive data - or to install malware–capable of granting remote control access, stealing information or spying–on the user's device. The attacker sends an email or other electronic message, often by pretending to be a trusted individual or organization, to a user, requesting information or a file download. If the user responds with the information or downloads the file, their security is compromised.

While phishing often uses vague language and references, spear-phishing attacks are highly-tailored to the individual who is being targeted, and therefore require prior research in order to be effective[1]. Like traditional phishing attacks, spear-phishing is also meant to steal sensitive information or infect a device or a computer network with malware that can monitor the device for sensitive information[2].

All types of phishing attacks rely on social engineering, the use of psychological manipulation to trick people into revealing confidential information. Spear-phishing tends to be more convincing, and therefore more successful, than generalized phishing attacks. Spear-phishing attacks can be connected to advanced persistent threats (APT), the consistent and hidden monitoring of an individual or an organisation for the purpose of having access to confidential information that can be exploited[3].

Spear-phishing comes in different forms: emails with links or attachments, a message on social media channels, or a message in a chat application.

---

[1] https://sec.eff.org/topics/phishing-and-malware

[2] Giandomenico, Nena "What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing" *Digital Guardian* https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing 24 October 2019 (Date accessed: 12 April 2020)

[3] "What's Worse: APTs or Spear Phishing?" *InfoSec Institute* https://resources.infosecinstitute.com/whats-worse-apts-or-spear-phishing/ 25 September 2015 (Date accessed: 12 April 2020)

Spear-phishing attacks in Ukraine

The Digital Security Lab (DSL) in Ukraine shared two notable incidents of spear-phishing in an interview with researchers from The Engine Room.

The first attack happened in November 2019, when an investigative journalist and the head of an organisation working with people in Occupied Crimea became the targets of a spear-phishing campaign on Facebook. Further investigation with Internews revealed that the attempt was likely an Advanced Persistent Threat (APT), rather than a one-off attack. In this specific case, the two individuals involved were able to recognise the spear-phishing attempt and report it to DSL.

The second case occurred in December 2019 when four groups of activists were sent targeted emails. For example, those who were interested in “music” received emails from a music group, asking them to write for a column. By February 2020, the attack was on-going. In the first two weeks of that month, eleven people had received spear-phishing messages. By the time of the interview, the total had increased to fifteen. According to DSL, the common adversary between these activists was local law enforcement, but they cannot make a clear attribution of the attack based on the “indicators of compromise” (emails, IP addresses, and other data that can point to the perpetrator). DSL further mentions that, “various features - emails, domains and IPs used, phishing code, used social engineering techniques, etc. - indicate that there is one group behind the campaign. It differs from the previously identified phishing campaigns against public activists by the style of execution and the specific choice of its objectives”.

Detecting spear-phishing

A report published by DSL in the first quarter of 2020 describes the different ways Ukrainian activists have been targeted through spear-phishing and non-targeted phishing messages. Non-targeted phishing attempts were deployed on the following platforms:

- Facebook: The target will receive a private message with a link to sites where they can vote for contests or watch personal videos. The link takes the user to a phishing site which asks for the target’s Facebook log-in and password. In January, DSL detected at least two cases of non-targeted phishing through Facebook private messages.
- Google Calendar: The target will receive a Google Calendar invitation where the description of the event contains a link to a phishing site.

In comparison, a spear-phishing attack that uses prior knowledge about the targeted person is harder to detect than a general phishing attack. Generally, a spear-phishing message references information an individual has shared on social media and appears to come from a trusted source.

Such attacks usually take the form of an email with a malicious link or an attachment. Clicking on a link will take the target to a site that looks legitimate and will ask for the user's credentials (username, email, and passwords). Opening the attachment will install malicious software (malware) that can be programmed to infect either the device or the entire network that the computer is connected to. Once infected, the malware can continue to monitor the target for useful information about their activities.

In the first example described above, the journalist was able to detect the spear-phishing attack because she had previously attended a digital security workshop hosted by DSL in the past. The training she received gave her the tools to identify the suspicious message and report it to the DSL.

Since DSL is well-trusted among activists in Ukraine, the targeted activists felt safe in reaching out to them for support.

Impact of a spear-phishing attack

In the first example, according to DSL, the two individuals felt confident that the messages were spear-phishing attempts and reported it. This is a best case scenario, as organisations can't prevent phishing attacks, only improve how they react when they receive them.

The second case DSL shared had a larger negative impact on the activist community for a variety of reasons. The specificity of the email's personalised content and the number of targets implicated by the campaign contributed to an atmosphere of insecurity and anxiety. Activists targeted by the spear-phishing attack were concerned that the accounts and the personal information of their colleagues might also become compromised. There were also concerns that attacks carried out in the digital sphere might escalate to physical threats or assaults.

According to DSL, the spear-phishing attacks may have also been intended to intimidate the activist community and create an environment of mistrust.

Once a spear-phishing attack is detected, there are far-reaching consequences across implicated professional and social structures. In the second example, the activists were anxious because no one knew exactly who had been compromised within the movement, community, network or group. Such uncertainty has been known to trigger the creation of silos and/or inner 'trusted' circles within a movement, community, network or group that can eventually lead to a breakdown of trust among different stakeholders within it.[4] This can be especially challenging for groups that are unable to organise in-person (for example, those organising in different cities or countries). Remote organising relies on digital communications, meaning that sensitive information can be more vulnerable to cyberattacks. Building an environment of trust in digital spaces also poses additional challenges for organisers. For groups that predominantly organise over the internet, the detection or suspicion of a spear-phishing attack will likely have a deeper impact on organising and trust-building in the long term.

DSL strategically responded to the series of attacks by publicly disclosing the spear-phishing attempts. In doing so, they created opportunities for other activists to learn about what had happened, discuss their concerns, swap ideas, and stymie attempts to sow distrust among the group.

The impact of a successful spear-phishing attack is even worse. It can be the start of an APT, whereby devices or networks are compromised with malware designed to monitor users for information that can be misused and exploited. A successful attack can also lead to more spear-phishing attacks that escalate in sophistication as the APT gathers more specific details about individuals and groups targeted.

While more research is needed to document and understand the psycho-social impacts of spear-phishing attacks on individuals and groups, they are specifically designed to manipulate their

[4] https://holistic-security.tacticaltech.org/chapters/prepare/1-4-team-and-peer-responses-to-threat.html

targets. Victims of spear-phishing attacks often report feelings of guilt for being 'tricked' into such schemes, as if they did something wrong. Some traditional digital security support methods have been criticised for blaming and shaming victims who unintentionally contributed to the success of a spear-phishing attack. It is important to remember that spear-phishing attacks are so effective because they deploy social engineering strategies (such as instrumentalizing a target's personal information) and manipulate the target's emotions.[5] In a 2014 article for the Telegraph, a spear-phishing attack victim wrote about their experience, and highlighted his feelings of anger and isolation following the accusatory reactions of commentators online.[6]

Mitigation strategies and tactics

Mitigation and response strategies work best with network and community collaboration. It only takes one individual within your group, network, community or movement to be compromised for a spear-phishing attempt to be successful.

Mitigation strategies should be shared quickly and widely among communities to slow the rate of compromise within a group.

1) There are some **basic digital security practices**[7] that can minimise the threat of spear-phishing on individual devices:

- Keep your operating system and all software updated. Most phishing malware exploits bugs in software. Having the latest version installed will reduce opportunities for malware to successfully infiltrate your system.
- Install and maintain antivirus and anti-malware software on your desktop and mobile devices. (Make sure the anti-virus and anti-malware is recommended by a trusted source!)
- Enable Two-Factor Authentication (2FA) or Multi-factor Authentication (MFA) wherever possible. Although not successful in all cases, MFA can add a second layer of protection. Even if a phishing attempt successfully steals your passwords, attackers may not gain access to your MFA code. Using a Universal 2nd Factor (U2F) Key is the most effective way to lock down an account.[8]
- Don't open unverified links and files. When in doubt, confirm with the sender on another channel that you trust. Ask them directly: did you send this email/message to me?

2) **Practice healthy suspicion and learn how to detect a spear-phishing message.** Over the past few years, spear-phishing messages have become more sophisticated and harder to detect. No matter how careful you are, it is likely that you may fall for a phishing attempt at some point. Security isn't about all or none, and preventing some attacks is better than nothing.

With this in mind, here are some red flags to watch out for:

---

5 Fisher, Dennis. "Phishers Play on Emotions to Fool Victims" https://duo.com/decipher/phishers-play-on-emotions-to-fool-victims 19 August 2019 (Date Accessed: 28 April 2020)

6 Hood, Stuart "How do you recover from a spear phishing attack?" https://www.telegraph.co.uk/men/the-filter/10892090/How-do-you-recover-from-a-spear-phishing-attack.html 25 June 2014 (Date accessed: 28 April 2020)

7 https://ssd.eff.org/en/module/how-avoid-phishing-attacks

8 https://www.yubico.com/solutions/fido-u2f/

- The message is unsolicited and without context. For example, if the message is from someone that you know but barely communicate with, and they send you a link or a file to download.
- The message is asking you to go to a website and update your information.
- The URL shown in the link is different to what is shown when you hover your cursor over it.

It is important to note that highly sophisticated spear-phishing attacks will not have these red flags. In those cases, organisations and individuals must find alternative ways to contact the supposed sender to confirm the authenticity of the message.

The Digital First Aid Kit is a collaborative effort of the RaReNet (Rapid Response Network) (https://www.rarenet.org/) and CiviCERT (https://www.civicert.org/) that seeks to help rapid responders, digital security trainers and tech-savvy activists better protect themselves and the communities they support against the most common types of digital emergencies. It can also be used by activists, human rights defenders, bloggers, journalists or media activists who want to learn more about how they can protect themselves against cyber threats and support others.

The Digital First Aid Kit provides support in assessing the authenticity of suspicious digital communications and offers advice on what to do with them through an open questionnaire you can find here: https://digitalfirstaid.org/en/topics/suspicious-messages/##

This tool will help you further diagnose the situation or to share the message with external trusted organizations that will provide you with a more detailed analysis of the potential threat.

3) **Share information about the spear-phishing strategy within your group, network, community or movement,** to prevent others from falling for the attack. Start by asking yourself what information could help other community members stop the spread of an attack. Discuss whether there are benefits to reporting the phishing message with peers and practitioners. If you decide to do so, be very careful not to share the message in a way that others can fall for the attempt. Sending screenshots is safer than forwarding the email.

4) **Preemptively implement processes within organisations for staff to report suspicious emails and messages**, and protocols for how to reduce harm in the event that the attempt is successful.

5) **If you suspect that a message is a spear-phishing attempt, there are three clear steps that you can take**:

1. Do not open any links or files attached to the message, or provide any information to the sender.
2. Verify the message's contents with the person using a different communication channel. Even in informal chat room conversations, if someone sends you an unknown link, ask them what it is before you click on it.
3. Report the incident to a digital security practitioner that you trust. They may be able to confirm if the threat is suspicious, or speak to similar occurrences from others. Reporting incidents to trusted organisational and digital security practitioners allows them to identify emerging trends and alert other groups that may be potential targets of the same attack.

7) **If you are a digital security practitioner who has been reached out to by an organisation**, caution them against opening any unknown links or files as a first step, then gather more information on similar incidents to evaluate if the phishing attack is targeted.

Access Now's Digital Security Helpline[9] Community Documentation[10] identifies these common indicators as things to consider when looking out for spear-phishing attacks:

- A personalised message containing information about the recipient, or other signs of social engineering.
- Clues in the language used in the message's text, especially if it's a dialect.
- Any indicators that the phishing campaign could be targeting activists or members of civil society.
- Attempts to gather information on the recipient (phone number, email address, login id).

In order to collect information about the potential attack from a suspicious sender, you can look for indicators of compromise through:

1. E-mails, messages or communications:
    a. Asking the partner organisation to share the complete email with you, including full headers and attachments.
    b. Investigating the intent of the message.
    c. If the message does not seem to be spam and has links or files attached to the email, capture any suspicious URLs and save the file in an empty storage device for further analysis. If the email does not have links or files and is not spam, investigate it as a potential social engineering email.
2. Network scanning and traffic analysis of the organization's internal network.
3. Analyzing suspicious processes on individual devices, such as suspicious open ports.
4. Analysing suspicious files and links -- experienced security practitioners can use hashing techniques on files to determine information about the malware. When searching for information about malicious links, only use the domain name, rather than the entire URL, so as to not tip off the adversary that the attack has been thwarted.[11]

If you need additional support during the process of collecting or analysing relevant information, or once you've finished doing so, connect with your local or regional community, the MISP project (https://www.misp-project.org/) or the Access Now Digital Security Helpline to assess next steps.

Further resources that can guide you through this analysis can be found in:

- The Access Now Digital Security Helpline Public Documentation (https://communitydocs.accessnow.org/), more specifically, in the sections "How to Recognize Spear-Phishing and What to Do" (https://communitydocs.accessnow.org/281-spear-phishing.html), and "Client Receives a Suspicious/Phishing Email" (https://communitydocs.accessnow.org/58-Suspicious_Phishing_Email.html).
- Instructions on how to share a complete email that includes full headers and attachments can be found in this content by The Computer Incident Response Center Luxembourg (CIRCL): https://www.circl.lu/pub/tr-34/.
- Network scanning resources by SAFETAG: https://github.com/SAFETAG/SAFETAG/tree/master/en/exercises/network_scanning
- Communities @ Risk, Targeted Digital Threats Against Civil Society (https://targetedthreats.net/), a report from 2014 by the Citizen Lab (https://citizenlab.ca), an interdisciplinary research laboratory based at the University of Toronto's Munk School of

[9] https://www.accessnow.org/help/
[10] https://communitydocs.accessnow.org/
[11] https://communitydocs.accessnow.org/363-Analysing_Suspicious_PDF_files.html

Global Affairs, that sheds light on an often overlooked digital risk environment. This report also includes examples of specific phishing and spear-phishing attacks examples (https://targetedthreats.net/media/5-Appendix.pdf).

8) **Beyond these specific prevention tactics, it is necessary for organisations to have a plan for dealing with suspected or confirmed spear-phishing attacks**. Every organisation should be able to answer the question: what will you do if you suspect that you are being targeted for spear-phishing? Below is a list of steps that will strengthen the resilience of an organisation as to whether these attacks in the future.

- Report and submit suspected spear-phishing messages to groups that can verify the attack for you. For example: DSL, Citizen Lab or the Access Now 24/7 Helpline. Reach out to a local and trusted digital security practitioner if you need help making connections with these groups.
- Undergo a SAFETAG audit. The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) is designed for at-risk small-scale and low-income groups. By participating in this auditing process, organisations can get a better sense of what their digital security risks are – from website vulnerabilities to device-level threats or network issues.
- Share your suspicions about spear-phishing with your wider network and movement. You might find that similar organisations are experiencing the same thing, and together, you can develop a community response strategy.
- Acknowledge that spear-phishing attacks are not just a technical issue. Anxieties or feelings of fear among those who suspect that they have been compromised, or know someone that has been, has to be dealt within a trusting and safe environment. Acknowledge that these threats can contribute to a breakdown of trust within a community or movement, and work with each other to address this possibility.

Other considerations

Beyond digital security strategies and tactics, it is important for victims of spear-phishing, and their communities to not blame themselves for the consequences of cyber attacks. Spear-phishing tactics are rapidly evolving – today's known warning signs and protection methods may quickly become obsolete. This is one of the reasons why spear-phishing is so effective and hard to detect. It is important for those who have been victims of spear-phishing to realise that that attack was designed to trick them specifically. It is not their fault. It is equally important for those around the individuals who have been compromised to acknowledge this.

Critically, the community around those who have been compromised by spear-phishing attacks should take care not to ostracise victims. The groups around them should find ways of connecting with them to show support following the attack. Perhaps, in ways that do not involve the tools that spear-phishing attackers used, and in ways that extend beyond digital communication.

Resources

- Surveillance Self-Defense How-to: Phishing and Malware
  https://sec.eff.org/topics/phishing-and-malware
- Surveillance Self-Defense How-to: Avoid Phishing Attacks
  https://ssd.eff.org/en/module/how-avoid-phishing-attacks
- https://digitalfirstaid.org/en/topics/suspicious-messages/

- Six Common Phishing Attacks and How to Protect Against Them
  https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
- Spear Phishing Prevention Services in 2020
  https://www.wibidata.com/spear-phishing-prevention/
- Best Defense Agaisnt Spear Phishing
  https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html
- How to Detect Phishing Attempts
  https://blog.malwarebytes.com/101/2017/06/somethings-phishy-how-to-detect-phishing-attempts/
- Guide of response for a scenario where an organisation receives a suspicious phishing email
  https://communitydocs.accessnow.org/58-Suspicious_Phishing_Email.html