Attack Archetype

Sphear-Phishing

Internews


Internews

Table of Contents

Introduction

This attack archetype describes a specific form of phishing that targets a single individual, a single organization, or a set of similar entities. The essence of a phishing attack in general is sending a message to the victim that pretends to be legitimate communication, but with the ulterior motive of stealing sensitive information such as account numbers, usernames, passwords, or other credentials and data.[1] The most commonly encountered phishing attacks are commodity attacks that target large numbers of victims indiscriminately. These have, for the most part, criminal financial motivations. The attack this archetype focuses on, spear-phishing[2], however, is much more narrow. These attacks are often politically motivated and carried out directly or indirectly by a nation state with the goal of oppression, intimidation, suppression, or espionage.

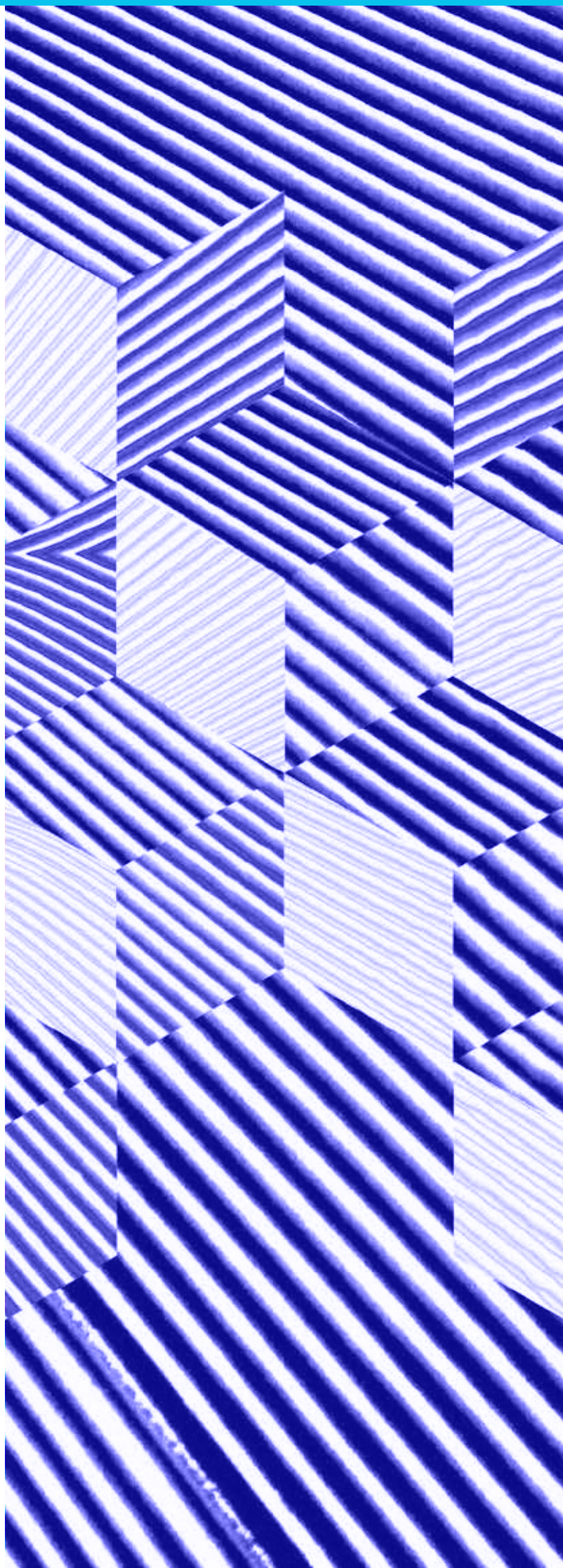
Types of Attack

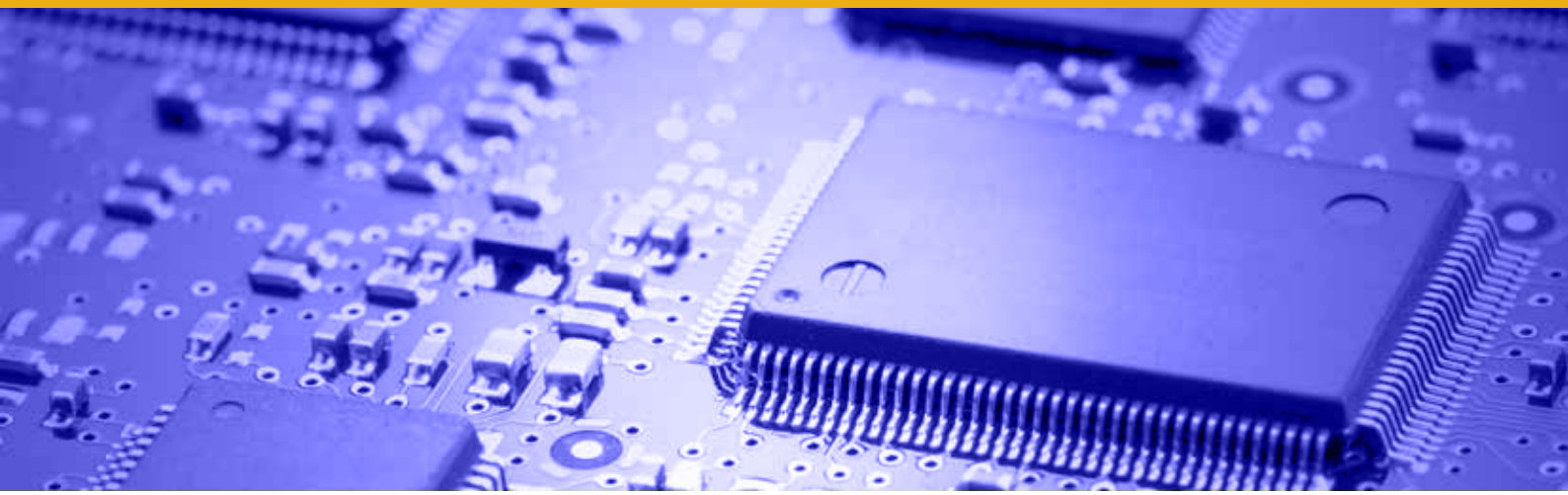
Spear-phishing can take a few different forms, differentiated by the means of communication used to transmit the phishing message. Less common forms of phishing are SMS phishing (smishing) and voice phishing (vishing). A more common form on the rise is phishing over a third-party service such as social media or messenger app.[3] The most common form of phishing is over email. This is the type which comes to mind first when someone thinks of phishing. Phishing over email can then be divided into two sub-categories: links and attachments. Phishing via links is the meth-

1 https://en.wikipedia.org/wiki/Phishing

2 https://attack.mitre.org/techniques/T1598/

3 https://attack.mitre.org/techniques/T1598/001/





od of the overwhelming majority of attacks. A phishing link is a URL embedded in some way in an email message that is designed to lure the victim into clicking the link and subsequently entering credentials or information into a website that is masquerading as a legitimate site.[4] Alternatively, the less common phishing attachment is typically a form or document that the victim is asked to complete and send back to the adversary.[5] The focus of the archetype outlined here is specifically phishing links tra`nsmitted over email, the most commonly encountered type of attack.

Targeted Individuals and Organizations

Spear-phishing can affect any type of organization or any specific individual, but according to the 2020 Microsoft Digital Defense Report, "nation state activity is significantly more likely to target organizations outside of the critical infrastructure sectors. The most frequently targeted sector has been non-governmental organizations (NGOs), such as advocacy groups, human rights organizations, nonprofit organizations, and think tanks focused on public policy, international affairs, or security."[6]

Social, Political, and Economic Context

The context around a particular spear-phishing campaign can be used to determine the adversary-victim relationship. According to the Diamond Model of intrusion analysis, this relationship is the social-political axis of the diamond.[7] There are two main components of an attack that this context can inform. The first is the motivating factors behind the attack. There may be an event that has occurred within the region or area within which the victim operates. Additionally, the adversary may be seeking to suppress information or silence speech about a particular event. Alternatively, the goal may be to steal information from the victim to be used at a later point in time for intimidation, harassment, doxxing, or influence operations. Separated somewhat from motivating factors, the second component of an attack that context can help inform is the topic used in the phishing lure itself. If there is a persistent, long-term adversary relationship with the victim, an event can be used to make the text of a phishing email or attached document more enticing. Information or documents surrounding a topic or happening of particular interest to a victim are often used to draw their attention and add a veneer of legitimacy to the lure.

4 https://attack.mitre.org/techniques/T1598/003/

5 https://attack.mitre.org/techniques/T1598/002/

6 https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738

7 https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Community Context

Careful attention to and communication about spear-phishing attacks can help prevent further attacks once one has been identified. If one organization or individual within a community is targeted by a spear-phishing attack, other related individuals or organizations may be targeted by the same adversary at the same time or shortly afterwards. For example, spear-phishing campaigns in the real world are often observed to target multiple individuals or organizations with similar roles. If the journalistic focus, or beat, of journalists from different organizations is the same, those different individuals may be targeted by a single spear-phishing campaign from one adversary. Similarly, if the focus of a set of civil society organizations are the same or similar, it follows that they are often targeted by the same set of adversaries using the same techniques all in a single campaign of spear-phishing emails.

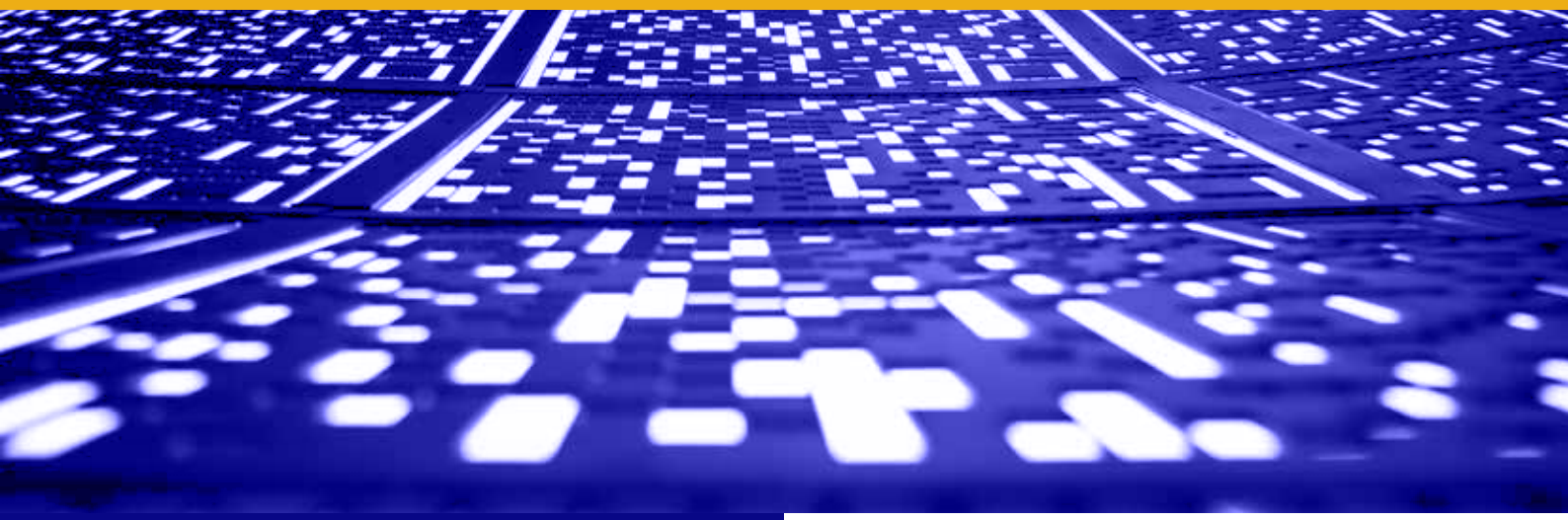
It's critical for organizations and individuals within spheres of civil society to communicate amongst one another about attacks that are occurring.

This can help detect and identify new attacks and prepare targets to be ready when one arrives at the inbox.

Attack Impact

The impacts of a successful spear-phishing attack can vary depending on the information or access that the adversary is able to acquire in the attack. The level of sophistication of this type of attack is so high that understanding what these impacts are for a specific individual or organization is crucial to controlling the damage when an attack is successful. Knowing that this type of attack will happen and planning how to recover from the attack is important in addition to defending against the attack in the first place.

Two processes that will help prepare for an attack are threat modelling and tabletop exercises. Threat modelling is the process of identifying all the assets of an individual or organization such as computers, networks, and accounts and then theorizing as to what type of adversary would attack each asset and how they would attack. Each asset is also analyzed to identify known and potential vulnerabilities, such as lack of second factor authentication for a particu-



lar account. These three factors – asset, adversary, and vulnerabilities – are then used to assign a risk score to each asset. Finally, these scores are used to help prioritize defensive efforts to the highest risk assets, knowing that resources are limited.

The second process that can help prepare for an attack is to run tabletop exercises. These are discussions of a set of plausible attack scenarios where one games out exactly what steps they will take to respond to a particular scenario. These exercises can help identify gaps in preparedness as well as potential specific impacts to the organization or individual.

Some of the most worrisome impacts of an attack can include, but are not limited to, the following:

- Downloading all emails from the victim's account.
- Using the victim's email address to launch subsequent spear-phishing attacks on people in their contact list.
- Using the victim's email account to reset passwords on other accounts that are tied to that address.
- Accessing other accounts which reuse the same password as the one stolen in the attack.
- Publicly posting in social media or publishing blogs or articles as the victim.

Process of the Attack

The basic steps of a spear-phishing attack are generally the same from one attack to the next. The steps in this process as applied to a fictitious human rights organization are as follows.

- Adversary performs reconnaissance on the victim by collecting publicly available information such as role within an organization, contact email address, and associated colleagues' names and information.
- A news event in the geographic area of the victim emerges.
- The spear-phishing email is crafted as an invitation to read a sensitive document about this event that is being shared by the victim's colleague via Google Drive.
- The link in the email is hosted on a domain that is very similar to a real Google Drive file sharing link.
- The victim clicks the link and is brought to the spear-phishing landing page.
- The page is nearly identical to a Google account login page including the victim's actual Google account avatar collected during the reconnaissance phase and embedded into the page.

- The victim enters their Google account login credentials.
- The adversary then uses these credentials to access the victim's email account.
- After collecting any emails from the account, the adversary uses the access to send a spear-phishing email to a subsequent victim who is in the original victim's contact list.
- The second victim detects that the email is malicious and reports it to their IT person. This report is communicated back to the original victim who then starts the response and recovery process.
- The first step in the response and recovery process is to identify all accounts that the victim owns and update passwords and credentials.
- Subsequent steps in the process are determined by specific asset types and follow a cycle of containment, eradication, and recovery.[8]

In addition to standard forms of spear-phishing attacks that are composed of a single email with an embedded URL, there are other frequently used techniques, such as the use of a beacon URL. Many email clients will load remote content automatically. An example of the benign use of this feature is an image in a person's email signature that is loaded from a URL rather than from an image embedded in the email as an attachment. Alternatively, and more closely to how adversaries use this feature, is marketing emails. There is often a hidden image or content loaded from a URL. This is still a benign use of the feature, but the goal is the same as when an adversary uses it: to reveal to that the email has been opened. This type of beacon can appear in the form of a read

8 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

receipt which is a built-in feature of many free email services. A more dangerous form of beacon is a URL hosted on systems that are fully under the control of the adversary. In this case, the adversary knows not only that the victim has opened the email, but also information about the victim's computer and location, which are based on the content of the packets sent to the adversary's system along with the IP address that they were sent from.

Another novel technique is the use of two or more separate emails sent to the victim. The earlier emails may contain no malicious links or content at all. They are simply a form of social engineering that are used to prepare the victim for a later malicious spear-phish. A concrete example of this would be a first email that seems to accidentally have not included an attachment or link. The phishing follow-up email then either contains an apology and the malicious content or a demanding question asking why the victim has not looked at the content sent in the previous message along with a message urging the victim to visit a URL to view said content.

A key and common component of spear-phishing attacks is forgery of email header data. Due to features in the protocol used to transmit emails, the From header field can be easily forged. As a result, emails can appear to come from a familiar email address but are actually sent by an adversary. Well-resourced adversaries can perform reconnaissance ahead of an attack to determine the identity, email address, and relationship with the victim that another individual or organization has that the adversary will masquerade as. A civil society organization may use a specific web developer, for example, and the spear-phish may be forged to appear to come from that developer's email address. The content of the lure in this case can be tailored to the relationship that the developer has with the victim to therefore appear authentic.

Prevention

Adversary techniques such as using a phishing follow-up email and the general attack of spear-phishing itself can be prevented by education and awareness.

Keeping an eye out for suspicious aspects of a particular email is very important. Also, using alternative forms of communication such as a phone call to confirm the authenticity of an email can prevent many attacks of this type.

In addition to general and awareness-based mitigations, concrete technical steps can be taken to prevent the two specific techniques of beacon URLs and "From" forgery. For beacon URLs, many email clients have a setting that can disable automatic loading of external content. Some email clients have a middle-ground setting between safety and usability that simply adds a step to loading external content that is then initiated by the user rather than the process being automatic. In the case of forgery of the From header field, an email authentication policy and reporting protocol called Domain-based Message Authentication, Reporting & Conformance[9] (DMARC) should be implemented on the mail server, if the individual or organization runs it themselves. If they use a third-party email provider, this should be part of that service. One of the specific goals of DMARC is to prevent this exact type of header forgery.

9 https://dmarc.org/wiki/FAQ


Internews