CAPEC-163: Spear Phishing (Version 3.9)

Archived: 2026-04-05 20:46:59 UTC

Attack Pattern ID: 163 **Abstraction: Detailed**		

Description

An adversary targets a specific user or group with a Phishing (CAPEC-98) attack tailored to a category of users in order to have maximum relevance and deceptive capability. Spear Phishing is an enhanced version of the Phishing attack targeted to a specific user or group. The quality of the targeted email is usually enhanced by appearing to come from a known or trusted entity. If the email account of some trusted entity has been compromised the message may be digitally signed. The message will contain information specific to the targeted users that will enhance the probability that they will follow the URL to the compromised site. For example, the message may indicate knowledge of the targets employment, residence, interests, or other information that suggests familiarity. As soon as the user follows the instructions in the message, the attack proceeds as a standard Phishing attack.

Likelihood Of Attack

High

Typical Severity

High

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type
ChildOf	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack
CanFollow	M Meta Attack Pattern - A meta level attack pattern in CAPEC is a decidedly abstract characterization of a specific methodology or techni
CanFollow	D Detailed Attack Pattern - A detailed level attack pattern in CAPEC provides a low level of detail, typically leveraging a specific techniq
CanFollow	S Standard Attack Pattern - A standard level attack pattern in CAPEC is focused on a specific methodology or technique used in an attack

This table shows the views that this attack pattern belongs to and top level categories within that view.

View Name	Top Level Categories
Domains of Attack	Social Engineering
Mechanisms of Attack	Engage in Deceptive Interactions

Execution Flow

Explore

1. **Obtain useful contextual detailed information about the targeted user or organization:** An adversary collects useful contextual detailed information about the targeted user or organization in order to craft a more deceptive and enticing message to lure the target into responding.

Techniques
Conduct web searching research of target. See also: CAPEC-118.
Identify trusted associates, colleagues and friends of target. See also: CAPEC-118.
Utilize social engineering attack patterns such as Pretexting. See also: CAPEC-407.

Collect social information via dumpster diving. See also: CAPEC-406.
Collect social information via traditional sources. See also: CAPEC-118.
Collect social information via Non-traditional sources. See also: CAPEC-118.

Experiment

1. **Optional: Obtain domain name and certificate to spoof legitimate site:** This optional step can be used to help the adversary impersonate the legitimate site more convincingly. The adversary can use homograph attacks to convince users that they are using the legitimate website. Note that this step is not required for phishing attacks, and many phishing attacks simply supply URLs containing an IP address and no SSL certificate.

Techniques
Optionally obtain a domain name that visually looks similar to the legitimate site's domain name. An example is www.paypaI.com vs. www.paypal.com (the first one contains a capital i, instead of a lower case L).
Optionally obtain a legitimate SSL certificate for the new domain name.

2. **Optional: Explore legitimate website and create duplicate:** An adversary creates a website (optionally at a URL that looks similar to the original URL) that closely resembles the website that they are trying to impersonate. That website will typically have a login form for the victim to put in their authentication credentials. There can be different variations on a theme here.

Techniques
Use spidering software to get copy of web pages on legitimate site.
Manually save copies of required web pages from legitimate site.
Create new web pages that have the legitimate site's look at feel, but contain completely new content.

3. **Optional: Build variants of the website with very specific user information e.g., living area, etc.:** Once the adversary has their website which duplicates a legitimate website, they need to build very custom user related information in it. For example, they could create multiple variants of the website which would target different living area users by providing information such as local news, local weather, etc. so that the user believes this is a new feature from the website.

Techniques
Integrate localized information in the web pages created to duplicate the original website. Those localized information could be dynamically generated based on unique key or IP address of the future victim.

Exploit

1. **Convince user to enter sensitive information on adversary's site.:** An adversary sends a message (typically an e-mail) to the victim that has some sort of a call to action to get the user to click on the link included in the e-mail (which takes the victim to adversary's website) and log in. The key is to get the victim to believe that the message is coming from a legitimate entity trusted by the victim or with which the victim or does business and that the website pointed to by the URL in the e-mail is the legitimate website. A call to action will usually need to sound legitimate and urgent enough to prompt action from the user.

Techniques
Send the user a message from a spoofed legitimate-looking e-mail address that asks the user to click on the included link.
Place phishing link in post to online forum.

2. **Use stolen credentials to log into legitimate site:** Once the adversary captures some sensitive information through phishing (login credentials, credit card information, etc.) the adversary can leverage this information. For instance, the adversary can use the victim's login credentials to log into their bank account and transfer money to an account of their choice.

Techniques
Log in to the legitimate site using another user's supplied credentials.

Prerequisites

None. Any user can be targeted by a Spear Phishing attack.

Skills Required

[Level: Medium]

Spear phishing attacks require specific knowledge of the victims being targeted, such as which bank is being used by the victims, or websites they commonly log into (Google, Facebook, etc).

Resources Required

An adversay must have the ability communicate their phishing scheme to the victims (via email, instance message, etc.), as well as a website or other platform for victims to enter personal information into.

Consequences

This table specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Confidentiality	Read Data	
Accountability Authentication Authorization Non-Repudiation	Gain Privileges	
Integrity	Modify Data	

Mitigations

Do not follow any links that you receive within your e-mails and certainly do not input any login credentials on the page that they take you too. Instead, call your Bank, PayPal, eBay, etc., and inquire about the problem. A safe practice would also be to type the URL of your bank in the browser directly and only then log in. Also, never reply to any e-mails that ask you to provide sensitive information of any kind.

Example Instances

The target gets an official looking e-mail from their bank stating that their account has been temporarily locked due to suspected unauthorized activity that happened in a different area from where they live (details might be provided by the spear phishers) and that they need to click on the link included in the e-mail to log in to their bank account in order to unlock it. The link in the e-mail looks very similar to that of their bank and once the link is clicked, the log in page is the exact replica. The target supplies their login credentials after which they are notified that their account has now been unlocked and that everything is fine. An adversary has just collected the target's online banking information which can now be used by them to log into the target's bank account and transfer money to a bank account of the adversary's choice.
An adversary can leverage a weakness in the SMB protocol by sending the target, an official looking e-mail from their employer's IT Department stating that their system has vulnerable software, which they need to manually patch by accessing an updated version of the software by clicking on a provided link to a network share. Once the link is clicked, the target is directed to an external server controlled by the adversary or to a malicious file on a public access share. The SMB protocol will then attempt to authenticate the target to the adversary controlled server, which allows the adversary to capture the hashed credentials over SMB. These credentials can then be used to execute offline brute force attacks or a "Pass The Hash" attack.

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping (also see parent)

Entry ID	Entry Name
1534	Internal Spearfishing
1566.001	Phishing: Spearfishing Attachment
1566.002	Phishing: Spearfishing Link
1566.003	Phishing: Spearfishing via Service
1598.001	Phishing for Information: Spearfishing Service
1598.002	Phishing for Information: Spearfishing Attachment
1598.003	Phishing for Information: Spearfishing Link

Content History

Submissions		
Submission Date	**Submitter**	**Organization**
2014-06-23 (Version 2.6)	CAPEC Content Team	The MITRE Corporation
Modifications		
Modification Date	**Modifier**	**Organization**
2017-01-09 (Version 2.9)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2017-08-04 (Version 2.11)	CAPEC Content Team	The MITRE Corporation
	Updated Attack_Phases, Attacker_Skills_or_Knowledge_Required, Description Summary, Examples-Instances, Resources_Required	
2018-07-31 (Version 2.12)	CAPEC Content Team	The MITRE Corporation
	Updated Attack_Phases, Related_Attack_Patterns	
2019-04-04 (Version 3.1)	CAPEC Content Team	The MITRE Corporation
	Updated Example_Instances, Related_Attack_Patterns, Taxonomy_Mappings	
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Example_Instances, Execution_Flow, Taxonomy_Mappings	
2020-12-17 (Version 3.4)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Attack_Patterns	
2022-09-29 (Version 3.8)	CAPEC Content Team	The MITRE Corporation
	Updated Taxonomy_Mappings	

2023-01-24 (Version 3.9)	CAPEC Content Team	The MITRE Corporation
	Updated Related_Weaknesses	

More information is available — Please select a different filter.
