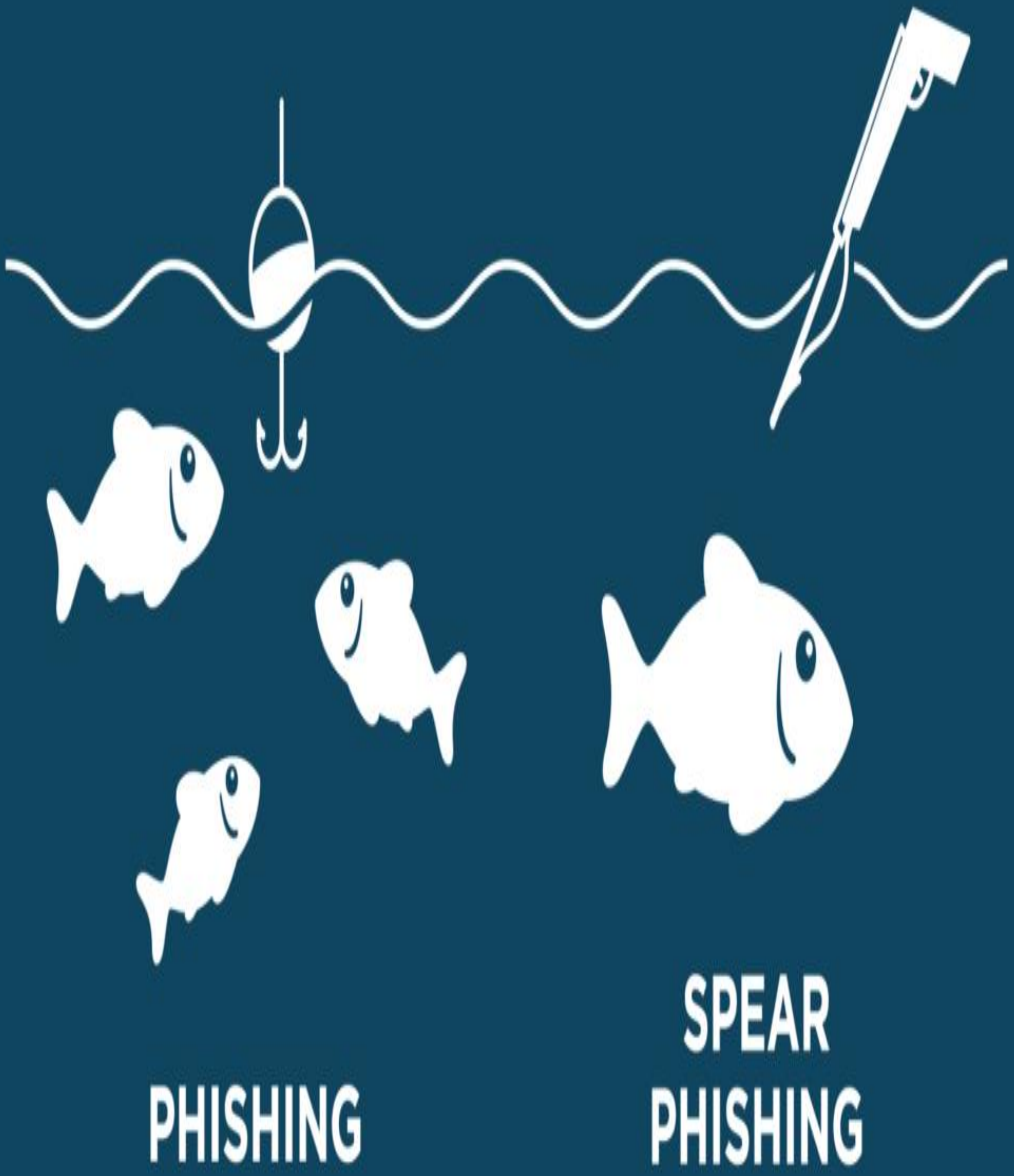
Spear Phishing: MFA’s Achilles’ Heel



Abstract:

Multifactor Authentication (MFA) or Second Factor Authentication (2FA) has been regarded as a strong security measure for protecting sensitive information and systems. However, this research paper shows a significant way to evade MFA through spear phishing attack used by the modern and advanced attackers to not only to infiltrate into the email accounts but to ex-filtrate the organization's critical data or to deploy malwares or specifically the ransomwares, etc. and educate the audience to protect the advance phishing attacks.

Introduction:

Multi-factor authentication is proven to be a powerful security measure to counter the rapidly increasing attacks against the traditional authentication methods such as single factor authentication. These old-school password-based authentication are susceptible to various attacks such as brute-force, SQL injection, confusion attacks, etc. and hence attacker's leverage these ways to compromise the end-user accounts to perform malicious activities.

MFA complements user's identification by adding an extra layer of security by requiring the end users to provide the evidence of their identity by incorporating additional factors along with username and password. such as biometric data (fingerprint, facial recognition), hardware tokens, SMS codes, or push notifications.

Now let's discuss in below section some of the basics of authentication with regards to MFA.

Authentication:

Authentication is the process for verifying the user's identity to establish the trust and ensure that only the authorized users are granted the access to the requested resources or information.

Authentication plays a vital role in protecting the sensitive information, securing the individual and organization's accounts, systems, and networks. Authentication is being setup for the users to ensure the complete privacy of the information and protection against the leaking of confidential data.

The authentication protocol is employed in almost all the digital domains such as banking, e-commerce, email services, social media platforms, corporate environment, and government systems.

Therefore, a proper authentication protocol should be setup properly because a misconfigured authentications can lead to breach of confidentiality, integrity, and unavailability of the digital resources.

In addition to the above secure configurations, it is also very important to educate the end-users against the modern phishing attacks to safeguard their digital resources and accounts.

Now, let's look at the below pictorial graphical representation of authentication to resource access –

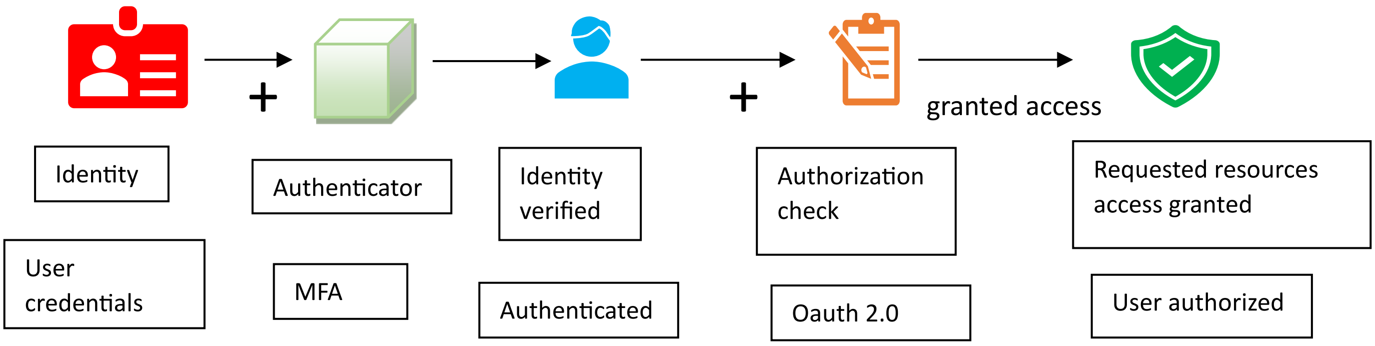


Fig i) – Authentication and Authorization to access the requested resources

Let’s dig down the above pictorial representation by defining certain parameters.

Identity:

Identity refers to the unique characteristics or attributes in both digital and physical world to identity the individual entity from others. In physical world the attributes to identify any user is via name, age, sex, nationality or National ID. However, in digital world username (generally some ID, or email address) and password refer as credentials to identify the end-user who is requesting the access to required digital resources.

Multi-factor token authentication:

MFA is also known as the access control token, which is associated uniquely with the user’s account, which the user upon entering the correct credentials along with the requested access control token, then the server upon verifying the whole HTTP/s request grants a session token to the user in form of Cookies which are stored at the user or the client end.

There are multiple authenticator access control apps available in the market such as Google Authenticator, Microsoft Authenticator, etc. these authenticator apps scan user’s identity in form of a digital barcode that stores the user’s information. Once the Authenticator apps verifies the user’s information and then grants the user an access token that keeps in active state generally for 60 secs.

Now let’s explore the mechanism of MFA via the pictorial representation.

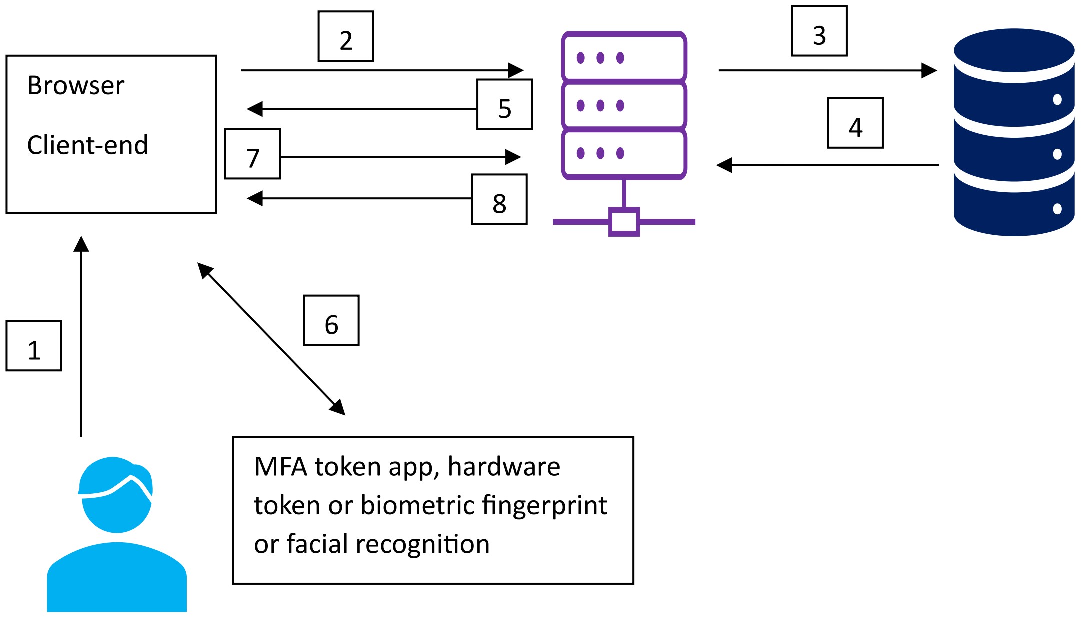

Browser
Client-end
1
2
3
4
5
6
7
8
MFA token app, hardware token or biometric fingerprint or facial recognition

Fig ii) Working of MFA

Let’s thoroughly discuss the aforementioned visual representation of how the MFA works:

1. User enters the username and password in the web application at client-end.
2. The browser will send the username and password to the web server in hash format.
3. The web server will check the hash in the stored database to verify if the user exists. This step is called the first factor authentication.
4. Once the verification or first factor authentication is completed, the database will send the success or failure message to the web server.
5. The web server will then send a challenge response to the user for the access control token.
6. The user will then enter the 2FA or MFA access control token.
7. The request containing the 2FA and challenge request with authentication response to the webserver.
8. The web server will verify all the details and then grants user the access to the resources and grants the user a session token generally in the form of Cookies.

Authorization:

Authorization is the process of granting the user an access to the certain resources by verifying certain attributes of the users. Now-a-days a very popular algorithm **Oauth2.0** is used in granting the access rights to the resources by providing the session token or cookies to retain the user session till the authentication expires.

Point to remember that the process of Authentication is not same as the process of Authorization.

Now there are 2 ways to define the authentication such as **In-band** and **Out-of-band** authentication.

In-band authentication – is a type of authentication method in which the authentication process occurs at the same communication channel.

For example – in online banking if both the credentials and recovery answer is to enter in the same communication channel, here that is browser.

Out-of-band authentication – is a type of authentication method in which one factor of authentication is via one channel and another factor is via different channel.

For example – the user set of credentials are being communicated over browser and the access code is sent via SMS or Authenticator apps.

Now as we can see that the MFA authentication is always a better way of authenticating the user and providing an access, as single factor authentication is susceptible to numerous authentication bypass attacks.

Benefits of MFA:

1. Higher security
2. Fraud prevention to some extent
3. Higher efficiency
4. Greater flexibility
5. Better productivity
6. Reduced operating

Hacking into MFA:

This section of the research paper demonstrates the emerging attacks on bypassing the MFA and compromising the victim accounts.

In order to hack into the victim account, the attackers look into the entire process of MFA from Identity to authentication, then the access control tokens and in last the session cookies. The most prominent hacks include, SQL Injection, brute-force, session replay, session hijacks, Cross-Site Scripting and many more.

Generally, there are multiple ways that attackers target victims to bypass the MFA:

1. MFA misconfigurations
2. Social Engineering
3. Phishing
4. Session Hijacking
5. Brute-force
6. Altering the MFA token itself
7. Banco Trojan, etc.

However, this paper will concentrate on the spear phishing and MFA misconfigurations.

Part I Spear Phishing:

Spear phishing is a form a targeted phishing attack which aims to trick the specific individuals usually the corporate employees such as HR, Finance, IT etc. by sending the personalized, legitimate emails or SMSs. Spear phishing is not like the traditional phishing, which sends the emails to wider audience with a hope of tricking the victims, but spear phishing focuses on the specific target to exploit with the certain individualities, interests, or associations.

In spear phishing, the attacker does extensive research about the target via social media platforms, dorks, search engines, websites, leaked information, dark web, etc. to gather the critical information such as names, email addresses, internal information, IDs, departments, job titles, etc.

Now, based on the collected information, the attacker crafts a very sophisticated email or message to send it to the actual target or the target's colleague or a more trustworthy resource such as manger, or for personal attack kids, wife, parents, etc.

Spear phishing relies often on social engineering techniques to trick the users to click on the malicious HTML links resulting in compromising the user accounts, hijack user sessions, hijack session cookies, downloading malicious files, or leaking confidential information. These actions result in unauthorized access to corporate or organization's systems, financial loss, brand loss, ransomware attack or bring down the whole organization's infrastructure.

Now let's explore the mechanism of spear phishing to compromise the user's account protected via 2FA.

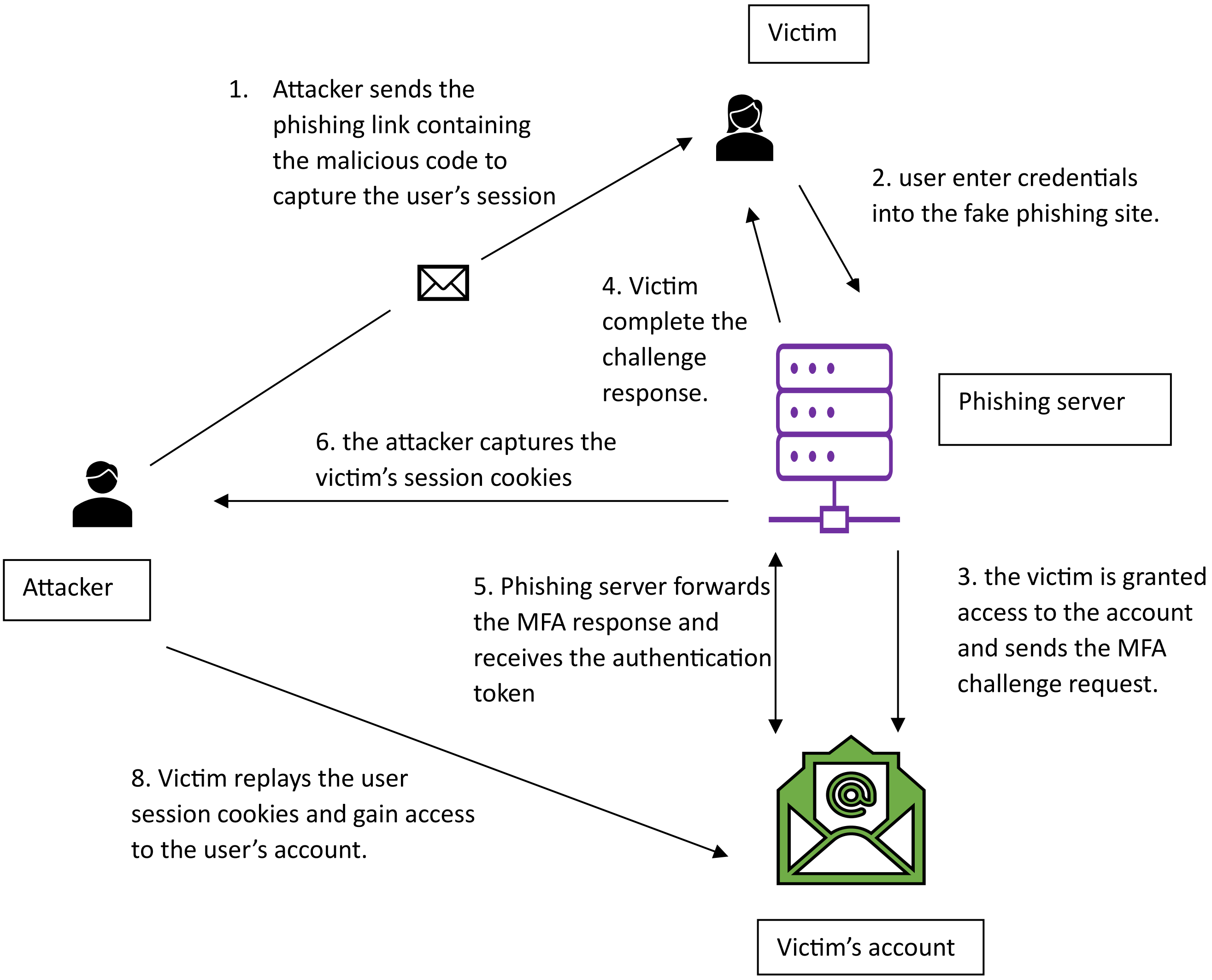

Victim
1. Attacker sends the phishing link containing the malicious code to capture the user's session
2. user enter credentials into the fake phishing site.
4. Victim complete the challenge response.
Phishing server
6. the attacker captures the victim's session cookies
Attacker
5. Phishing server forwards the MFA response and receives the authentication token
3. the victim is granted access to the account and sends the MFA challenge request.
8. Victim replays the user session cookies and gain access to the user's account.
Victim's account

Fig iii) Spear Phishing bypassing MFA

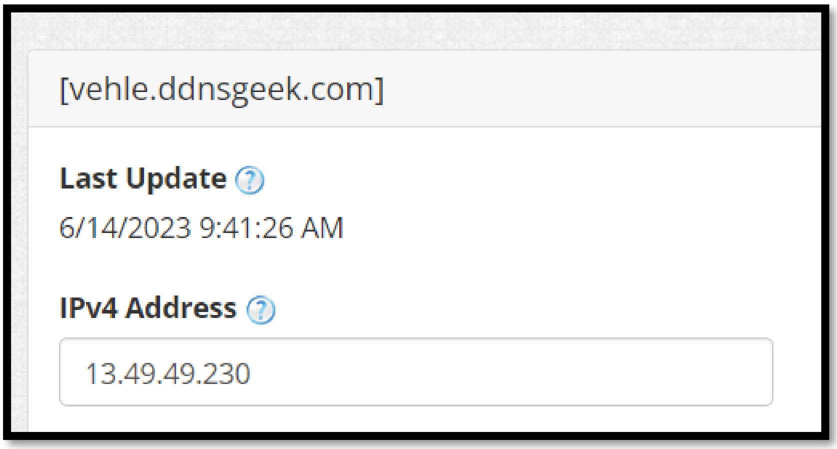
Now, let's look at a practical demonstration of the above demonstrated attack through the provided screenshots below, illustrating the step-by-step process of the spear phishing attack.

Step 1: Download the evilgnix2 from the below link:

Download Evilginx2

Note – to install and configure the evilgnix2 framework is straightforward, and hence we will be skipping this particular part.

Step 2: Now make sure the phishing domain is setup to point the A records to the phishing server, as shown in the following screenshots:

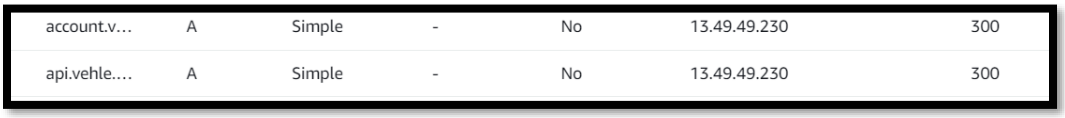


[vehle.ddnsgeek.com]

Last Update
6/14/2023 9:41:26 AM

IPv4 Address
13.49.49.230

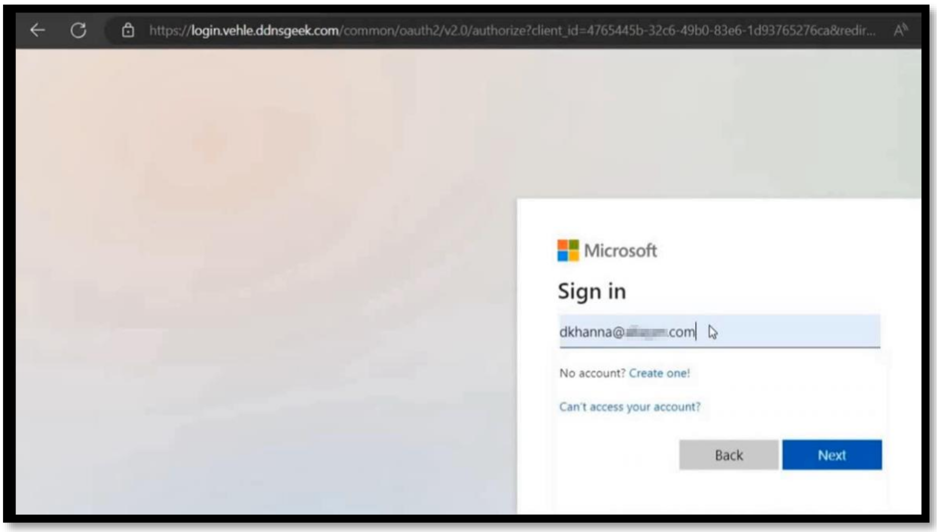
Step 3: Once the domain is setup, make sure to setup the Route53 subdomain pointers to the EC2 public IP address, samples are shown as below:



account.v...	A	Simple	-	No	13.49.49.230	300
api.vehle....	A	Simple	-	No	13.49.49.230	300

Step 4: Now, fire up the evilngix2, and load the phishlet. Once the phishlet is loaded, setup the lures to generate the phishing URL.

Step 5: Now send the phishing URL to the victim, as shown in the following screenshot.



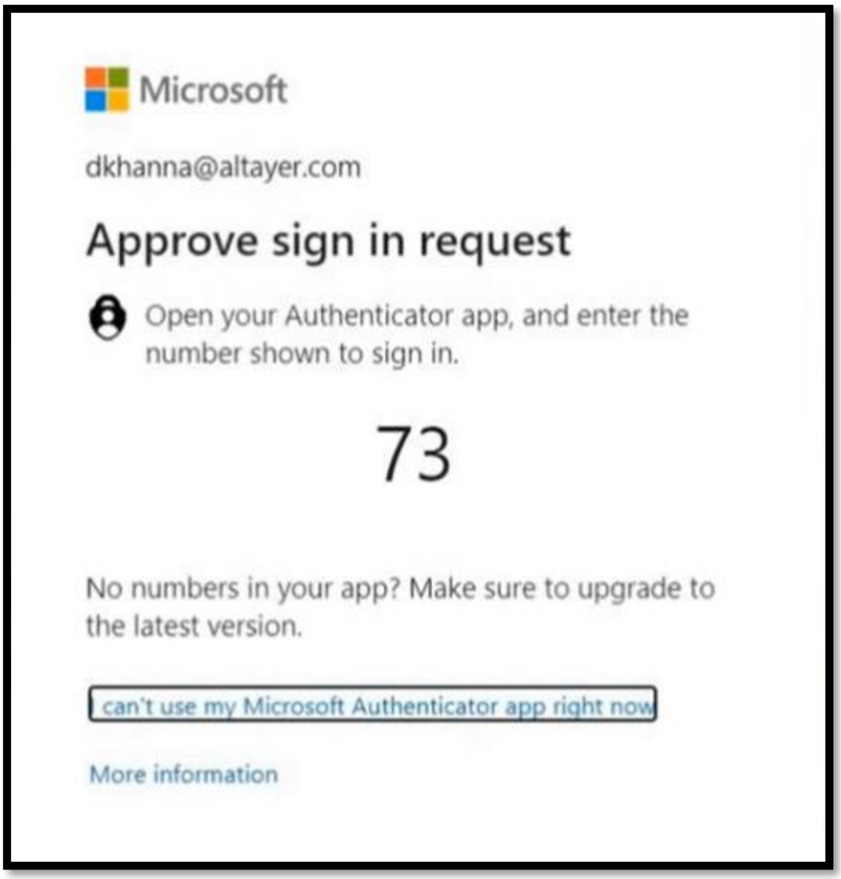
https://login.vehle.ddnsgeek.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redir...

Microsoft

Sign in

dkhanna@[redacted].com

Step 6: Now once the victim enters the password, the server will send the request to Authenticator for MFA challenge response. Once the victim approves the MFA challenge, the attacker will receive the session cookies of the victim, as shown in the following screenshots:



Microsoft

dkhanna@altayer.com

Approve sign in request

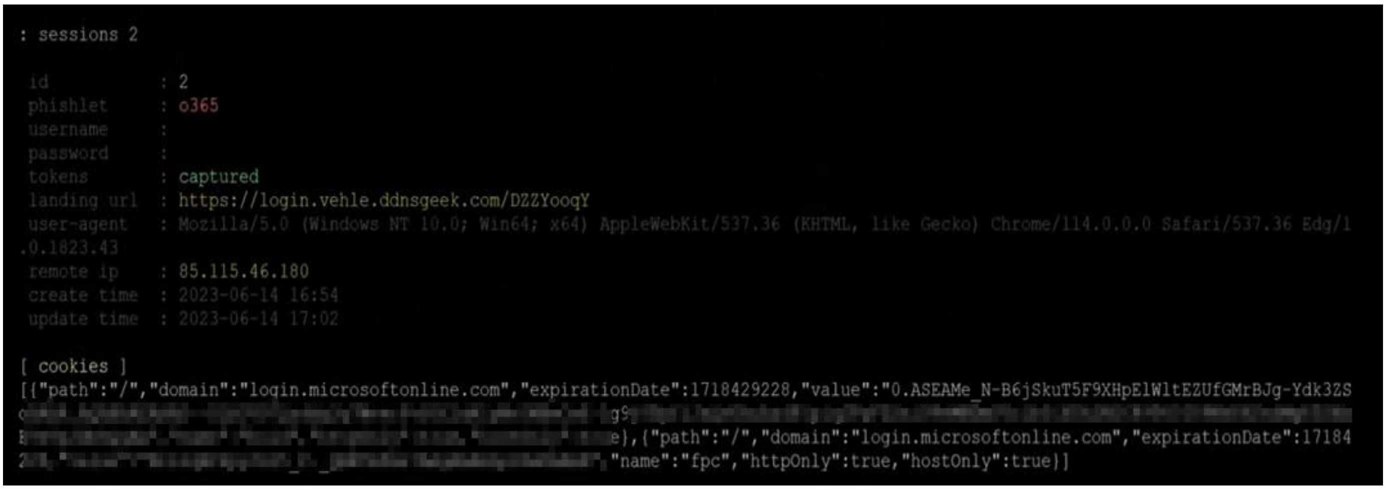
Open your Authenticator app, and enter the number shown to sign in.

73

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

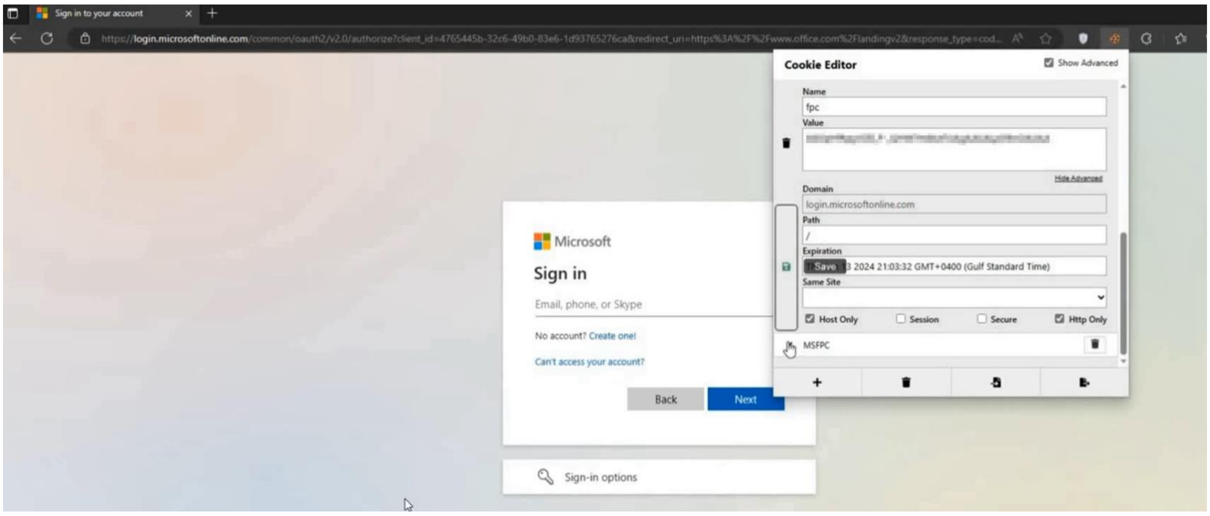


```
: sessions 2

 id           : 2
 phishlet     : o365
 username     :
 password     :
 tokens       : captured
 landing url  : https://login.vehle.ddnsgeek.com/DZZYooqY
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/1
.0.1823.43
 remote ip    : 85.115.46.180
 create time  : 2023-06-14 16:54
 update time  : 2023-06-14 17:02

[ cookies ]
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1718429228,"value":"0.ASEAMe_N-B6jSkuT5F9XHpElWltEZUfGMrBJg-Ydk3ZS
[redacted]g[redacted]
[redacted]e},{"path":"/","domain":"login.microsoftonline.com","expirationDate":17184
[redacted]"name":"fpc","httpOnly":true,"hostOnly":true}]
```

Step 7: Now, let's copy the cookies and using the cookie editor replace the cookies with the captured cookie, as shown in the following screenshot.



https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=cod...

Cookie Editor ☑ Show Advanced

Name: fpc

Value: [redacted]

Hide Advanced

Domain: login.microsoftonline.com

Path: /

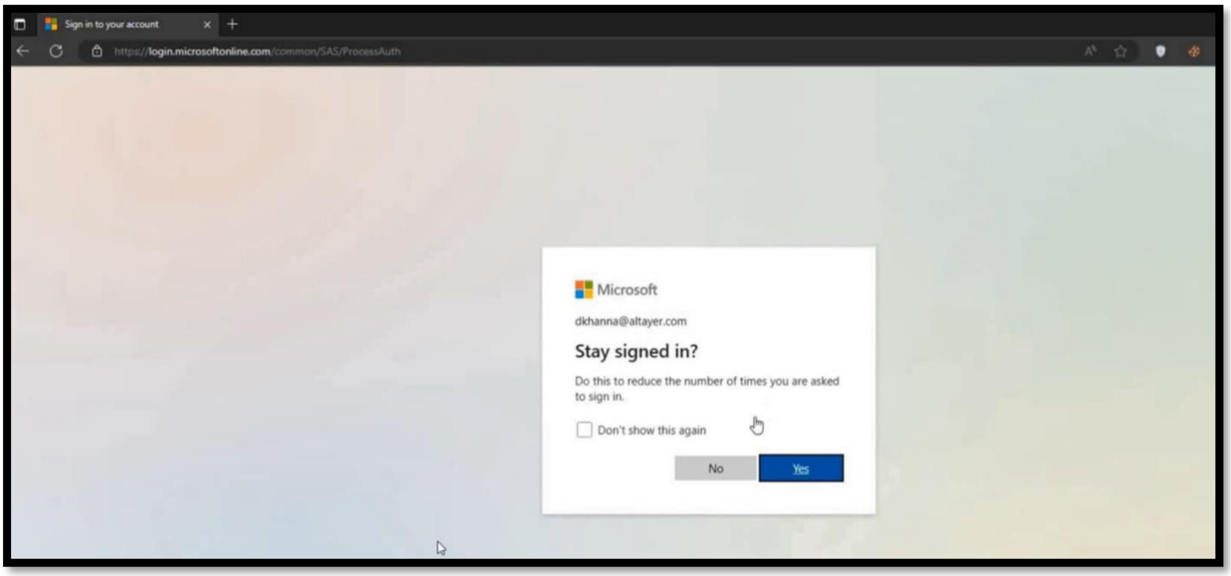
Expiration: 3 2024 21:03:32 GMT+0400 (Gulf Standard Time)

Same Site:

☑ Host Only ☐ Session ☐ Secure ☑ Http Only

MSFPC

Step 8: Now once the attacker refreshes the page, the cookies will let the attacker logs back in to the victim's o365 account, as shown in the following screenshot.



https://login.microsoftonline.com/common/SAS/ProcessAuth

dkhanna@altayer.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

Conclusion –

MFA is a widely accepted as an effective security measure, though it is not immune to exploitation. Sophisticated techniques such as spear phishing, misconfigurations, etc. attackers can target individuals and the organizations, trapping them into revealing their MFA credentials and gaining unauthorized access.

This research paper has shed light on the vulnerabilities and misconfigurations associated with MFA. By analysing real-world examples and conducting experiments, we have highlighted the potential flaws in MFA systems and the methods used by attackers to exploit them and gain unauthorized access to the victim's accounts.

To lower MFA bypass risks, organizations should take the below steps:

1. Implement a proper MFA authorization token like Authenticator.
2. Proactively check the configurations of the MFA.
3. Employees should be educated and awareness campaigns should be organized on regular basis regarding the emerging threats.
4. SIEM and other detections should be in place for unauthorized attempts and access.