MFA bypass via reverse Proxy

Hacker can login without credentials using OAuth2-Attacks / new AitM Attack

Introduction

In the past few days, cybercriminals used a variety of techniques for their OAuth attacks, such as OAuth2 Attacks. The sophisticated attacks sometimes even relied on Microsoft's own platform to generate invitations to the consent page for dangerous websites or applications.

OAuth-based application attacks frequently focus on senior management, account managers, human resources, and finance personnel—precisely the individuals with privileged access to extremely sensitive information. When such attacks are successful, malicious actors gain permanent entry to emails, files, contacts, notes, Microsoft Teams chats, and other valuable data. In certain instances, they may even redirect users to a phishing site subsequent to obtaining their consent to utilize the application.

During this kind of attacks (called AiTM), a phished user interacts with an impersonated site created by the attacker**. This allows the attacker to intercept credentials and session cookies and bypass multifactor authentication (MFA),** which can then be used to initiate other attacks.

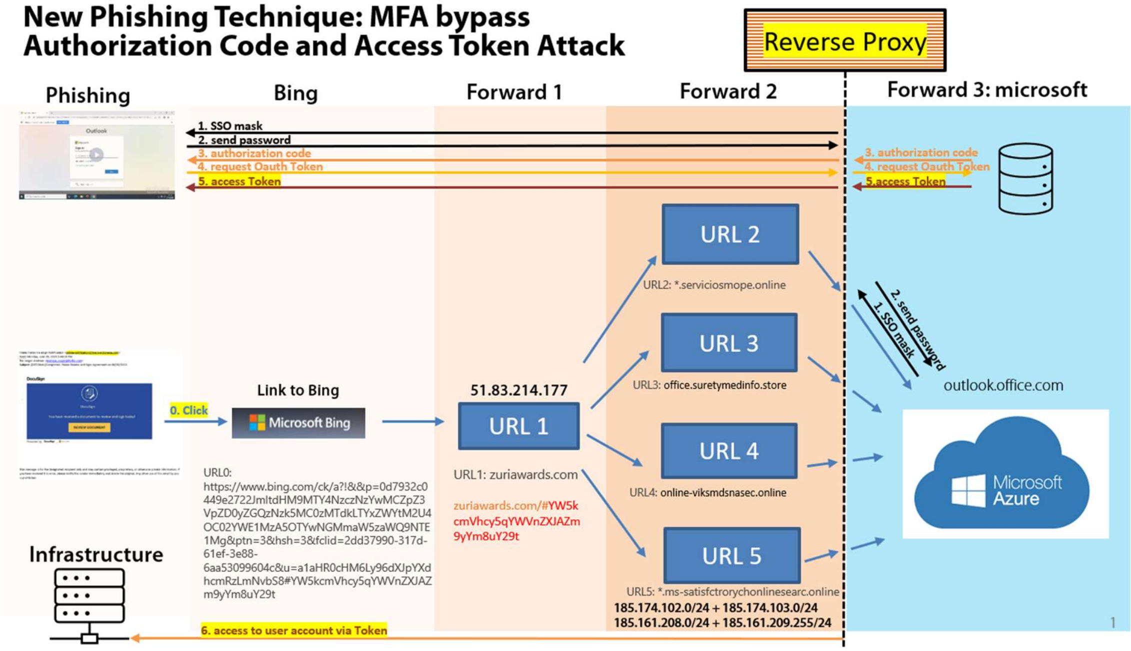
Oauth2 authentication

OAuth serves as a commonly utilized authorization framework that empowers websites and web applications to request limited access to a user's account on another application. A key advantage of OAuth is that it enables users to grant access to their account without disclosing their login credentials to the requesting application. Consequently, users have the ability to specify which data they wish to share, rather than relinquishing complete control of their account to a third party.

Basically, the vulnerability associated with OAuth revolves around the misconfiguration of the OAuth service itself, which can allow attackers to get authorization codes or access tokens linked to other users' accounts. **By acquiring a valid code or token**, attackers gain the potential to access the victim's data, leading to a complete compromise of their account. In fact, the attacker could potentially impersonate the victim user on any client application registered with the affected OAuth service. The specific mechanism depends on the grant type employed. In either case, a code or token is transmitted through the victim's browser to the "/callback" endpoint specified in the "redirect_uri" parameter of the authorization request.

The fundamental OAuth process finds widespread use in integrating third-party functionalities that necessitate access to specific user account data. For instance, an application may leverage OAuth to seek access to a user's email contacts list, enabling it to suggest potential connections. Additionally, this mechanism facilitates third-party authentication services, enabling users to log in using an account associated with a different website.

The hackers devised an exceptionally sophisticated method to "acquire" user credentials. I have presented the process through the following slides:


New Phishing Technique: MFA bypass
Authorization Code and Access Token Attack
Reverse Proxy
Phishing
Bing
Forward 1
Forward 2
Forward 3: microsoft
1. SSO mask
2. send password
3. authorization code
4. request Oauth Token
5. access Token
3. authorization code
4. request Oauth Token
5.access Token
URL 2
URL2: *.serviciosmope.online
URL 3
URL3: office.suretymedinfo.store
2. send password
1. SSO mask
outlook.office.com
0. Click
Link to Bing
Microsoft Bing
51.83.214.177
URL 1
URL 4
URL4: online-viksmdsnasec.online
Microsoft Azure
URL0:
https://www.bing.com/ck/a?!&&p=0d7932c0449e2722JmltdHM9MTY4NzczNzYwMCZpZ3VpZD0yZGQzNzk5MC0zMTdkLTYxZWYtM2U4OC02YWE1MzA5OTYwNGMmaW5zaWQ9NTE1Mg&ptn=3&hsh=3&fclid=2dd37990-317d-61ef-3e88-6aa53099604c&u=a1aHR0cHM6Ly96dXJpYXdhcmRzLmNvbS8#YW5kcmVhcy5qYWVnZXJAZm9yYm8uY29t
URL1: zuriawards.com
zuriawards.com/#YW5kcmVhcy5qYWVnZXJAZm9yYm8uY29t
Infrastructure
URL 5
URL5: *.ms-satisfctrorychonlinesearc.online
185.174.102.0/24 + 185.174.103.0/24
185.161.208.0/24 + 185.161.209.255/24
1
6. access to user account via Token

1. Phishing: Upon clicking, the victim is redirected to a Bing address.
2. Within a few milliseconds, the user is then redirected to a new URL where, depending on the Bing address, a new code via GET is added at the end of URL. This code is a sequence of number and contains the encrypted email address of the potential victim.
3. Following another few milliseconds, the victim is randomly redirected to a different website where the email address is decrypted. The hackers have maintained a pool of URLs, regularly adding new ones each day (Forward 2).
4. Lastly, the victim is redirected with the username as parameter to outlook.office.com, where is prompted to enter their access credentials.

As a final step, the user encounters the authentic login screen of Microsoft. However, upon entering their credentials, Microsoft sends a token back to the previous URL (controlled by the hacker). This token, serving as a random number for login purposes, grants the hackers the highest probability of accessing the data.

Possible mitigations

To enhance security and mitigate the types of attacks observed in the previous lab, it is considered a best practice for client applications to establish a whitelist of legitimate callback URIs during registration with the OAuth service. Consequently, when the OAuth service receives a new request, it can verify the redirect_uri parameter against this whitelist. If an external URI is provided, an error is likely to occur. However, it is important to note that there might still exist potential methods to circumvent this validation process. During the auditing process of an OAuth flow, it is advisable to conduct experiments with the redirect_uri parameter to gain a better understanding of its validation mechanism. For instance:

- If additional values can be appended to the default redirect_uri parameter, there is a potential opportunity to exploit inconsistencies in how the URI is parsed by various components of the OAuth service. For instance, you can attempt techniques such as:

- In some cases, you may encounter server-side parameter pollution vulnerabilities. As a precautionary measure, it is recommended to test by submitting duplicate redirect_uri parameters in the following manner:
  - https://URL2.com/?client_id=123&redirect_uri=outlook.office.com&redirect_uri=URL2/callback

Awareness

It is important to remain vigilant and cautious when interacting with emails, messages, or websites, particularly when they request personal information or involve sensitive transactions. Verifying the authenticity of the source, checking for suspicious indicators, and being cautious of clicking on unfamiliar links or attachments, can help prevent falling victim to phishing attacks.

MFA Bypass

In the following illustration, you will find a depiction of the TCP Protocol and the connections involved in the MFA bypass scenario.

After the initial redirect triggered by URL 1, the victim establishes connections to URL 2, 3, 4, or 5 through a Reverse Proxy. This proxy assumes control and monitors all TCP connections to and from URL 2, 3, 4, 5, and the Microsoft Portal.

The yellow dot indicates the moment when the proxy can capture the "Authorization code," while the red dot indicates when the proxy can steal the "OAuth Token." These tokens enable the hacker to log in as a user.

Using this technique, the hacker can circumvent common MFA Authentication systems such as SMS, Microsoft Authenticator, and potentially even FIDO Hardware authentication (e.g., yubikey).

Please consider that the presented scenario outlines a potential use of TCP/DNS Protocols to bypass MFA. It is important to understand that this a result of a "reverse engineering" to illustrate the possible connections. Please note that there is no guarantee that the connections and sequences depicted are exact or definitive.

Credit for reverse engineering: Dipl.El.Ing.ETH G.Moresi

Links:

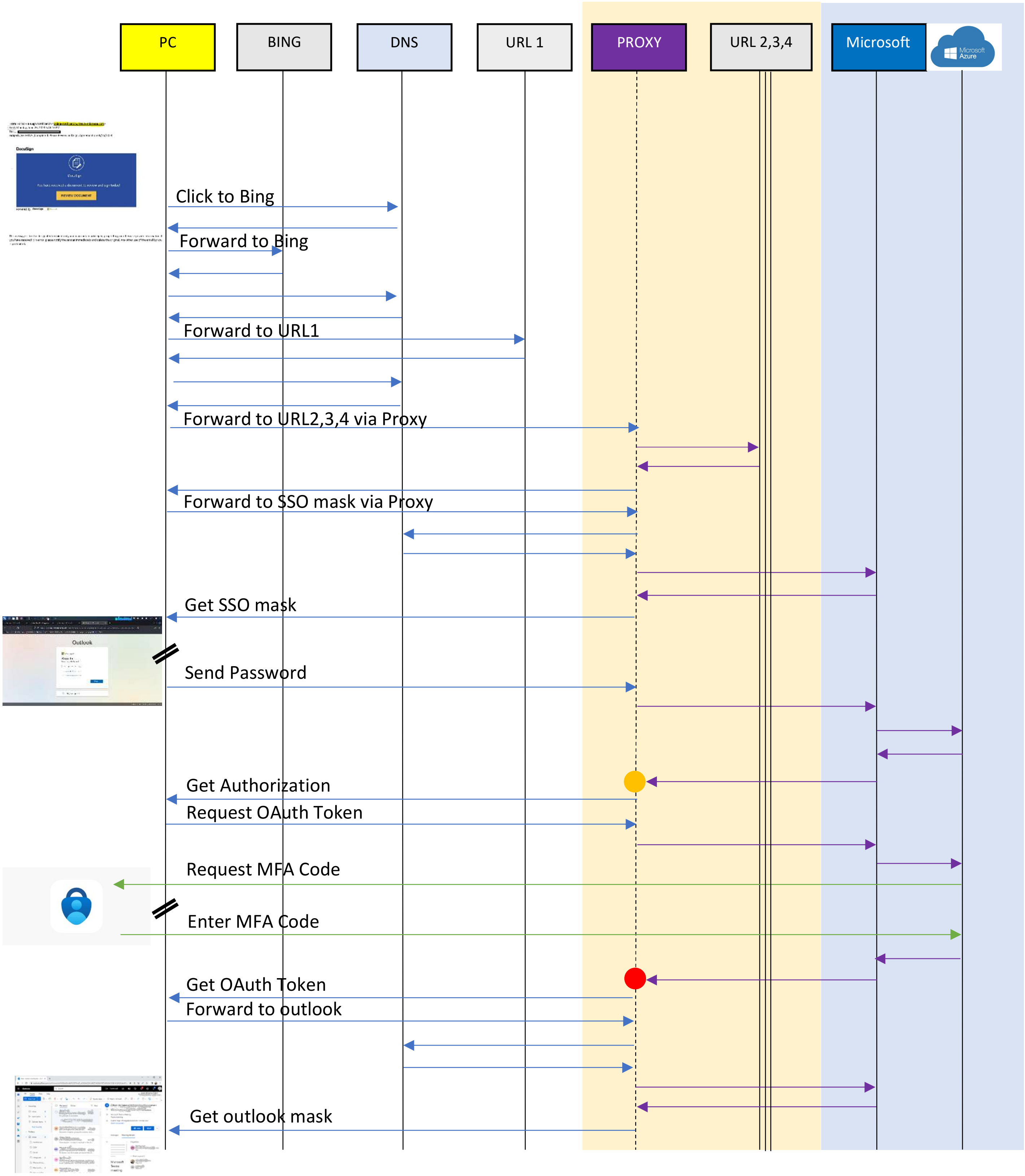
https://www.youtube.com/watch?v=d2qELe4z8Kw

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/automatically-disrupt-adversary-in-the-middle-aitm-attacks-with/ba-p/3821751

https://www.techrepublic.com/article/adversary-in-the-middle-phishing-campaign-bypasses-mfa-mimics-office/

https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

MFA bypass - Simplified TCP-UDP/DNS Protocol Flow – reverse Engineering (probable TCP flow)


PC
BING
DNS
URL 1
PROXY
URL 2,3,4
Microsoft
Microsoft Azure
DocuSign
REVIEW DOCUMENT
Click to Bing
Forward to Bing
Forward to URL1
Forward to URL2,3,4 via Proxy
Forward to SSO mask via Proxy
Get SSO mask
Outlook
Send Password
Get Authorization
Request OAuth Token
Request MFA Code
Enter MFA Code
Get OAuth Token
Forward to outlook
Get outlook mask