Implementation of advanced phishing Attacks and defences against them

By

Yash Nawghare(2671357)

Supervisor: Prof. Rishiraj Bhattacharyya
Inspector: Prof. Matthew Leeke

School of Computer Science

College of Engineering and Physical Sciences

University of Birmingham

2023-24

Abstract

For more than 2 decades years, Phishing attacks have always been one of the most dangerous. Throughout this period time adversaries are constantly evolving and developing new techniques to pass traditional security measures. Among them, Adversary-in-the-middle (AiTM) appeared to be one of the major threats. As it has been modified very recently, it is capable of passing through conventional detection systems and multi-factor authentication (MFA). In this project, I implemented AiTM phishing attacks in two ways, one is server-based methods and the other is serverless one. Then I tried to analyse how effective the current defence methods could be when it comes to AiTM attack.

The main reason of this research is to get a comprehensive while also an in-depth understanding of the ways in which AiTM phishing attacks operate. The implementation of AiTM was conducted in a situation where environments depend on MFA for user authentication. to carry out the assessment of the effectiveness of currently existing defence methods. The project uses open-source phishing toolkits like Evilginx, to simulate real-world attack situations. These simulations focus on two kinds of AiTM attack models. The first is the server-based method using Virtual Private Servers (VPS) while the other is the serverless method that uses cloud services like Cloudflare Workers. After deploying phishing sites that look the same as legitimate websites the attacks aim to capture user credentials, passwords and MFA session tokens, by passing through enabled security mechanisms

The methodology includes designing, configuring, and executing AiTM phishing attacks in controlled environments. The server-based attacks require setting up a phishing site on a dedicated VPS, a manually configuring DNS records, SSL certificates, and phishing toolkits. The serverless attack hand will use cloud-based functions to automate phishing operations with minimal infrastructure which will reduce detection rates also the operational costs.

Defence mechanisms are analysed and focused on anti-phish MFA solutions and certificate-based authentication. FIDO2 security keys, a hardware-based authentication method, are tested for their resilience against AiTM attacks. Also certificate-based authentication which will ensure only authorised devices can access services is also analysed for its ability to mitigate the risk of session token theft.

The findings show that there are not many important differences in the effectiveness of defence strategies against server-based and serverless AiTM phishing attacks. While traditional MFA methods like password and SMS-based authentication always remain vulnerable to AiTM attacks.Also more advanced solutions like FIDO2 and certificate-based authentication are strong protection. The project shows that serverless AiTM attacks, which use cloud which use temporary infrastructure are more challenging to detect and mitigate due to their temporary nature .

This project demonstrates that while AiTM phishing attacks present a major while also always evolving threat. Modern authentication solutions and defence mechanisms can provide effective mitigation.The difference of the two architectures is always been discussed .Also phishing infrastructure uses ,misuses and impact has been discussed.

Acknowledgements

I want to thank to all those who have helped and also guided me through the way of completing this dissertation. I would have not able to do this research without their support
Firstly ,I would like to thank my supervisor Prof . Rishiraj Bhattacharyya for his vital and important guidance also encourage me to positive push all the way through the project. His insightful feedback .solid support were very beneficial in the right direction of my research. Also helping me through different challenges during the research.

I am always thankful to all the faculty members of the School of Computer Science at the University of Birmingham for helping out and teaching solid foundation of knowledge that was very beneficial for me and my dissertation

I would also like to thank my family and friends, who always helped and supported me during hard times and helped me through challenging situations. Thank you all for supporting and always motivating me through this time

At last, I would also like to acknowledge the cybersecurity community and all the developers of the open-source tools that were helpful to me in my dissertation experiments and analysis. I will always appreciate their efforts and contribution to the cybersecurity community

I would also like to thank everyone who directly or indirectly contributed or helped me during my dissertation period.

Abbreviations

AITM	Adversary in the middle
MFA	Multi Factor Authentication
2FA	Two Factor Authentication
BEC	Buisness Email Compromise

List of Figures

Table of Contents

List of Figures

List of Tables

CHAPTER 1

1 Introduction

Phishing has always considered as a major threat for a long time. Users are always considered the weakest link of cybersecurity. Phishing takes advantage of the users. Phishing in the past involves deceiving attempts to gather sensitive information such as usernames, passwords, and credit card details by being as a fake honest entity in an important communication. The adversary (attacker/fake honest person) always keeps developing the methods of phishing. The introduction and use of multi-factor authentication (MFA) was seen as a beneficial step in order to protect online identities and sensitive data. But this did not discourage the adversaries, rather they always used different tactics and developed them to implement a more advanced attack which is hard to detect. This project aims to implementation of advanced phishing attacks specifically AiTM in a controlled and ethical manner. Also, two types of infrastructure were implemented The project also discusses the effectiveness of current security measures and the impact of the attack.

1.1 Background

Considering both personal or businesses,cyber-attacks are always a threat to them. Phishing is a type of social engineering attack which is widespread and always evolving day by day. It takes support of human nature and behaviour which result in difficulty to detect and mitigate. In the past years, phishing keeps evolving from fraud emails to bypass advanced authentication techniques like MFA.AiTM is a very good example of this evolved nature of phishing attacks.

AiTM involves an attacker who sits in between the communication of a user and an original service to catch or change the sensitive information that has been transferred. Traditional phishing can be mitigated by educating users to recognise and avoid fraudulent requests, sites etc . AiTM attacks exploit the real-time processing of communication and data transfers which will make them very difficult to detect,prevent and mitigate

1.2 Problem Statement

Although the defences are also developed, AiTM phishing attacks always remain very effective. These attacks compromise the confidentiality and integrity of very sensitive data and also ruin the trust in digital communication systems. The problem has worsened as there are open-source phishing kits available that can be misused very easily. That is why it is very important to understand and always stay aware of this kind of advanced phishing attacks.

1.3 Research Objectives

This project aims to achieve important objectives as follows:

- To implement simulated AiTM phishing attacks using both server-based and serverless architectures to understand their working and impact.
- To analyse different mitigation methods like phish-resistant MFA,certificate based authentication and their effectiveness
- Comparative analysis of server-based and serverless architecture ,uses and disadvantages

1.4 Research Questions

This project aims to answer the following question:

- How effective are AiTM phishing attacks in circumventing current security measures such as MFA?
- What are the specific vulnerabilities exploited by server-based and serverless AiTM attacks?
- Which defence mechanisms are most effective in mitigating the risks posed by these advanced phishing attacks?
- How can organisations better prepare and respond to the evolving landscape of phishing threats?

1.5 Scope of the Study

This research will focus on the implementation and analysis of AiTM phishing attacks within a controlled environment. The study will not cover other forms of phishing, such as voice phishing (vishing) or SMS-based phishing (smishing), although these are recognised as significant threats. The defences evaluated will be limited to those relevant to AiTM attacks, specifically targeting the interception authenticated tokens of Microsoft login.

1.6 Significance of the Study

The findings of this dissertation are intended to contribute to the broader field of cybersecurity by enhancing the understanding of AiTM phishing mechanisms and their effective countermeasures. By providing a detailed analysis of attack strategies and defence effectiveness, this study aims to inform better security practices and strategies for organisations and individuals alike. Additionally, it seeks to foster a more profound academic and practical understanding of the capabilities and limitations of current cybersecurity technologies in facing advanced phishing threats.

CHAPTER 2

2 Literature Review

2.1 History of Phishing and Evolution

Phishing started in mid 1990 which targeted AOL users with email scams. These attacks were comparatively not very complicated but used social engineering methods to deceive users to give out (Safi and Singh, 2023a)sensitive information. In the report by Kaspersky Lab, phishing was initially considered a minor threat which primarily affected the most new users. Over the years, phishing techniques have developed and become advanced. The Kaspersky report from 2011-2013 summarises how phishing evolved from basic email scams to advanced attacks which involved fake websites and advanced social engineering methods. These attacks often mimic original website like online banking services, to trick users into entering sensitive information (THE EVOLUTION, 1997)

In a systematic literature review by Benavides et al. (2020) summarises the evolution of phishing detection techniques, showing the transition from heuristic methods to machine learning and deep learning approaches. This change shows the increasing advancement of phishing attacks and the need for more advanced detection mechanisms.(Safi and Singh, 2023b)

Modern phishing attacks have diversified beyond email to include mobile phishing, voice phishing (vishing), and phishing on social media platforms. According to a LinkedIn article, these new methods exploit the widespread use of mobile devices and social networks, making it easier for attackers to reach a larger audience(Shaikh et al., 2016)

The study by Chanti and Chithralekha provides a comprehensive classification of phishing attacks, categorizing them based on the attack vector (email, social media, malware, etc.) and the target (individuals, organizations, specific industries). This classification helps in understanding the various forms of phishing and the specific challenges associated with detecting and preventing each type. (Chanti and Chithralekha, n.d.)Phishing attacks have evolved from simple email scams to sophisticated, multi-vector threats that require advanced detection and prevention methods and while significant advancements have been made ongoing research is essential to stay ahead of attackers and develop more effective anti-phishing strategies. These threats now use various channels and techniques making them harder to detect and prevent, and constant adaptation is necessary to combat these evolving tactics. Continued research not only improves current methods but also anticipates future challenges, ensuring a proactive approach to cybersecurity.

2.2 Emergence of AiTM Phishing

Adversary-in-the-Middle (AiTM) phishing represents a significant evolution in phishing tactics, designed to circumvent traditional security measures such as Multi-Factor Authentication (MFA) .
AiTM phishing attacks have become increasingly prevalent as threat actors seek to deploy stealthy, high-volume phishing attacks. According to SC Media, the rise in phishing-as-a-service platforms with AiTM functionality has facilitated the covert exfiltration of user credentials, session cookies, and two-factor authentication codes. This trend is driven by the need to bypass MFA defenses, which have become a standard security measure in many organizations(AiTM phishing attacks on the rise | SC Media, n.d.)

A detailed analysis by Microsoft Sentinel highlights the use of tools like Evilginx2, Modlishka, and Muraena in AiTM phishing campaigns. These tools act as intermediaries between the target and legitimate login portals, capturing authentication tokens and session cookies in real-time. This method allows attackers to gain unauthorized access to accounts even when MFA is enabled(Identifying Adversary-in-the-Middle (AiTM) Phishing Attacks through 3rd-Party Network Detection - Microsoft Community Hub, n.d.)

2.3 Current State of BEC Attacks

Financial Impact and Prevalence

Business Email Compromise (BEC) attacks have become one of the most financially damaging forms of cybercrime. The FBI reported that in 2022 alone, BEC attacks resulted in $2.7 billion in losses, with a significant increase of 81% in incidents compared to the previous year.(BEC Attacks in 2023: What Organizations Need to Know, n.d.)

The financial impact of these attacks continues to grow, with the FBI's Internet Crime Complaint Center (IC3) receiving approximately 21,500 BEC complaints in the past year, resulting in reported losses totaling $2.9 billion(The Weaponization Of AI: The New Breeding Ground For BEC Attacks, n.d.)
BEC attacks have evolved significantly over the years, becoming more sophisticated and harder to detect. Initially, these attacks involved simple impersonation techniques where attackers would pose as high-ranking executives or trusted partners to trick employees into transferring funds or sensitive information. However, modern BEC attacks now employ multi-stage strategies and leverage advanced technologies. BEC attacks target a wide range of industries, with the finance sector and logistics and fulfilment industry being particularly hard hit. The FBI has also warned that BEC attacks are now targeting food shipments, indicating that attackers are constantly finding new ways to exploit different sectors for financial gain.
)(Identifying Adversary-in-the-Middle (AiTM) Phishing Attacks through 3rd-Party Network Detection - Microsoft Community Hub, n.d.)

Modern BEC attacks are not limited to email. Attackers are now using various communication channels, including SMS text messages, voice calls, and messaging apps like Teams, Zoom, WhatsApp. (
This diversification makes it more challenging for organizations to detect and defend against these attacks. The increasing sophistication of Business Email Compromise (BEC) attacks poses significant challenges for detection and defence and traditional security measures such as email filtering and multi-factor authentication (MFA) are often insufficient against these advanced attacks. BEC attacks takes advantage of social engineering techniques to manipulate the victims into transferring money or revealing sensitive information by bypassing many standard security protocols. These attacks often involve imitating and carefully crafting messages that can deceive even old users. Therefore there is a desperate need for more advanced and adaptive security measures that can mitigate the developing tactics of BEC attackers. Which will help in better protection of organizations and the people

2.4 Tactics and Techniques

Modern BEC attacks are different due to adaptability and advancement. Attackers often impersonate as original business contacts or executives which will result in users revealing their sensitive information and resulting in a loss . This attack would not include malicious emails or users or anything unreal as it uses the original resources of a compromised organization. An alarming trend in BEC attacks is the interception of legitimate payments. Attackers will be acting as vendors and provide different payment instructions which will effectively redirect funds to their own accounts. This method has proven particularly effective, as it exploits existing business relationships and processes.

Multi-stage BEC attacks involve a series of coordinated activities which is designed to compromise email accounts and exploit them for financial gain. These attacks usually start with the compromise of a trusted vendor or partner organization. The attackers then use the compromised organization to launch AiTM phishing attacks, capturing credentials and session cookies from multiple organizations. Once they have access to the email accounts, they conduct follow-on BEC activities like sending fraudulent invoices or redirecting payments (Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog, n.d.)

2.5 Detailed Analysis of AiTM Phishing Techniques

Proxy Servers and Session Hijacking

AiTM phishing attacks leverage proxy servers to intercept and manipulate traffic between the user and the legitimate website. The attacker sets up a fake login page that mimics the legitimate site. When the user enters their credentials, the proxy server captures this information and forwards it to the legitimate site, allowing the attacker to hijack the session. This technique enables attackers to bypass MFA by capturing and replaying session cookies, granting them access to the victim's account without further authentication (Rising AiTM phishing attacks: how to protect against them | Chorus, n.d.)

2.6 Bypassing Multi-Factor Authentication (MFA)

With respect to MFA Aitm phasing can bypass it which is very concerning By capturing and replaying session cookies, attackers can gain access to user accounts without needing to complete the MFA process by their own. This capacity seriously compromises one of the main security systems companies depend on to stop illegal access. AiTM attacks' ability to overcome MFA has caused security plans to be reassessed. Companies are realising more and more that although MFA is still a vital security tool, it is not perfect and needs to be supplemented by other levels of defence. (How attackers can bypass MFA using AiTM, and how to defend against it | Claranet UK, n.d.)

2.7 Overview of Serverless Technologies in Cybersecurity

Benefits and Risks of Serverless Computing

Serverless computing is a cloud computing execution model where the cloud provider dynamically manages the allocation and provisioning of servers. This model offers several benefits, including scalability, cost-efficiency, and ease of deployment. Developers can focus on writing and deploying code without worrying about server management, leading to faster development cycles and reduced operational overhead (Introducing the Amazon Linux 2023 runtime for AWS Lambda | AWS Compute Blog, n.d.)

However, serverless computing also presents certain risks, particularly in the context of cybersecurity. The same characteristics that make serverless platforms attractive to developers also make them appealing to cybercriminals. Attackers can leverage serverless platforms to create low-footprint, scalable phishing infrastructures that are difficult to detect and mitigate. The temporary nature of serverless functions and the lack of proper infrastructure make it more challenging to monitor and secure these environments effectively ((Identifying Adversary-in-the-Middle (AiTM) Phishing Attacks through 3rd-Party Network Detection - Microsoft Community Hub, n.d.))

2.8 Serverless Platforms in Phishing Attacks

Serverless platforms like AWS Lambda, Azure Functions, and Cloudflare Workers are being increasingly used by cybercriminals to implement phishing attacks. These platforms allow attackers to deploy phishing infrastructures with minimum code requirement and less hassle. For example, Cloudflare Workers can be utilized to run JavaScript functions that intercept traffic between victims and legitimate login pages, facilitating the capture of credentials and session cookies(AiTM Phishing Attacks: Stolen Session Cookie Creates Havoc in Financial Organizations, n.d.)

2.9 Existing Research on AiTM Phishing

Studies and Reports by Microsoft

Many studies and reports have shown the growing threat of AiTM phishing attacks. Microsoft has been at the forefront of researching and mitigating these threats. Microsoft's Defender Experts uncovered a multi-stage AiTM phishing and BEC attack against banking and financial services organizations. The attack originated from a compromised trusted vendor and transitioned into a series of AiTM attacks and follow-on BEC activities. This attack demonstrated the complexity and evolving nature of AiTM and BEC threats.Another study by Microsoft Sentinel emphasized the importance of advanced monitoring techniques to detect and respond to AiTM phishing attacks. The report highlighted the use of reverse-proxy functionality and the role of third-party network logs in identifying the footprints left by these sophisticated attacks (Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog, n.d.)).

2.10 Gaps in Current Research and How This Dissertation Addresses Them?

Despite the growing body of research on AiTM phishing and BEC attacks, several gaps remain. Existing studies have primarily focused on the detection and mitigation of these attacks, with limited emphasis on the implementation and technical challenges involved in setting up AiTM phishing infrastructures. Additionally, there is a need for more comprehensive defense strategies that address both technical and organizational aspects of cybersecurity.This dissertation aims to fill these gaps by providing a detailed demonstration of a serverless AiTM phishing attack, highlighting the technical aspects and challenges involved. The research will be also evaluating the effectiveness of the attack in bypassing traditional security measures and analyze it

CHAPTER 3

3 Methodology

3.1Research Design and Approach

This project is designed to show and analyse server-based and serverless(Adversary in the middle) phishing attacks. It was made sure that the project was done in a controlled manner so that no real people would be affected. The setup of the project involves creating a phishing scenario by creating Microsoft Office business emails and fake users for testing. Evilginx was used for the server-based method and Cloudflare Workers and Slack workspace for the serverless method This resembles a real-world AiTM phishing attack which targets Microsoft 365 login credentials which was chosen due to its widespread use in organizations.

3.2Understand the Working of Aitm attack

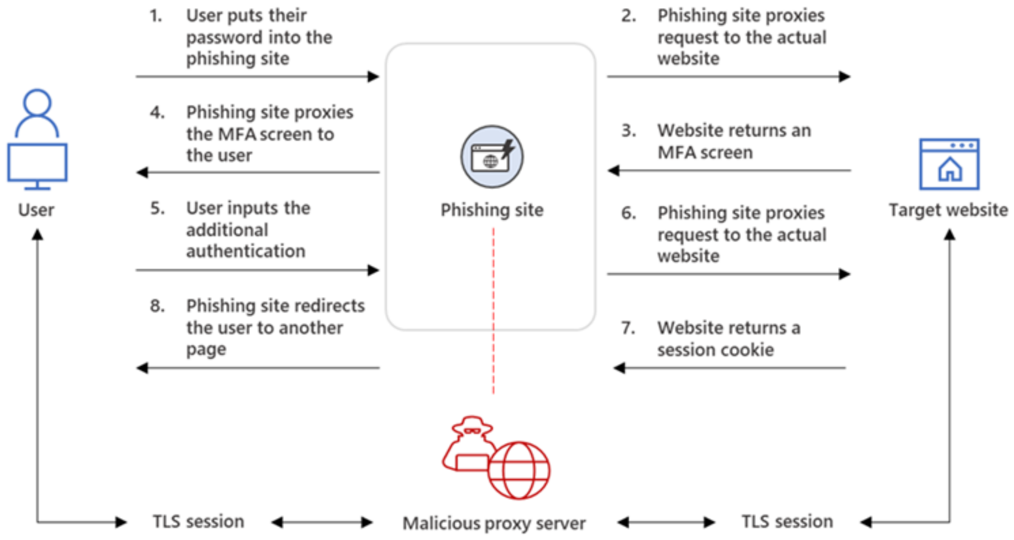

1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page
User
Phishing site
Target website
TLS session
Malicious proxy server
TLS session

Figure 1 : AiTM attack architecture by Microsoft(Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog, n.d.)

In modern web services user sessions are managed through session cookies, which are issued by an authentication service following a successful login. These cookies are used to validate a user's identity and maintain their session across more than one page visit that eliminates the need for repeated authentication. In Adversary in the Middle (AiTM) phishing attacks, an adversary targets these session cookies to bypass the authentication process entirely and impersonate the user .

The AiTM phishing attack is executed by setting up a proxy server that relays HTTP packets between the user and the target server. This proxy server hosts a phishing site designed to mimic the legitimate website. The key feature of this attack is the dual Transport Layer Security (TLS) sessions: one between the user and the phishing server, and another between the phishing server and the legitimate website. This setup allows the phishing server to intercept and relay requests and responses, including sensitive data such as authentication credentials and session cookies. (as shown in Fig 1.1)

In practice, the phishing site appears visually identical to the legitimate site, as all HTTP traffic is proxied through to the original website. The only difference is the URL, which reflects the phishing domain. By leveraging this method, attackers can capture the session cookies and other critical data without having to create a fake website from scratch.

Once the session cookie is obtained, the attacker can inject it into their own browser, effectively assuming the identity of the target user. This approach allows the attacker to bypass authentication measures, including multi-factor authentication (MFA), and gain unauthorized access.

3.3Understanding AITM attack with Tools(Server Based)

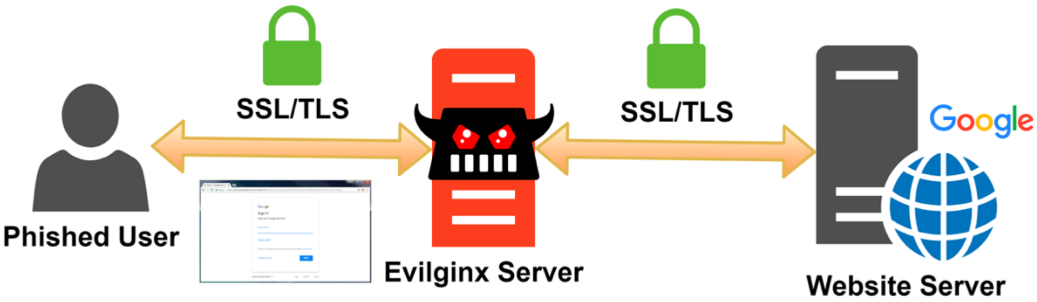


Figure 2 : Sever based architechture (Evilginx 2 - Next Generation of Phishing 2FA Tokens, n.d.)

The first step in an AiTM phishing attack is setting up a phishing site that completely resembles the legitimate website. Tools like Evilginx2, Modlishka, and Muraena make it easy **.**The attacker typically registers a domain that closely resembles the legitimate one . For example, a small difference (e.g., using "rn" instead of "m") can make the phishing domain look like a legitimate website . The attacker then configures DNS records to point to a server they control. To make the phishing site appear even more legitimate, the attacker uses these tools to automatically obtain SSL/TLS certificates from providers like Let's Encrypt. This gives the phishing site the "HTTPS" padlock, making it look secure to the victim. The tools use a reverse proxy to clone the legitimate website in real-time. This means that the phishing site isn't just a static copy—it mirrors the live, up-to-date content of the legitimate site, including all the forms and fields.

Once the phishing site is set up, the attacker needs to direct victims to it.Victims are usually fall to visit the phishing site through carefully crafted phishing emails, SMS messages, or social engineering tactics. These messages often contain urgent language or spoofed email addresses to make them look legitimate. When the victim clicks on the link, they are redirected to the phishing site that appears the same as the actual website they intended to visit.

The core functionality of AiTM tools comes into play when the victim interacts with the phishing site: The AiTM tool acts as a reverse proxy between the victim and the legitimate service. When the victim enters their login credentials on the phishing site, these credentials are immediately forwarded to the actual legitimate service.If the legitimate service requires MFA, the service sends a challenge (like a one-time password) back to the AiTM tool. The tool then relays this challenge to the victim, who enters the MFA code on the phishing site, unaware that it's being captured. Once the victim successfully completes the login and MFA process, the legitimate service sends a session cookie or token to the phishing site. This cookie is what the legitimate service uses to maintain the session without requiring re-authentication. The AiTM tool intercepts and stores this session cookie.With the session cookie in hand, the attacker can now gain unauthorized access to the victim's account: The attacker can use the captured session cookie to log into the victim's account on the legitimate service from a different device or location. This bypasses the need for credentials or MFA, as the session has already been authenticated. In many cases, attackers can maintain persistent access by using these session tokens until they expire. They might even use tools to refresh or extend session validity, ensuring ongoing access. To avoid raising suspicion, the phishing tool typically redirects the victim to the legitimate website after the session cookie is captured, or shows a generic error message. The victim may think they simply entered their credentials incorrectly or that the service is temporarily down.

3.4 Understand serverless AITM attack

Serverless computing platforms (such as AWS Lambda, Azure Functions, and Google Cloud Functions) allow developers to deploy code in the form of individual files or functions. These can be written in different types of programming languages like JavaScript, TypeScript, Python etc. These single-file applications are used for small tasks like handling HTTP requests and processing data. Serverless functions execute in response to events, such as HTTP requests. This makes them well-suited for handling real-time interactions. Functions do not maintain state between invocations, which means they are often used to perform short-lived tasks.

3.5Attack Architecture:

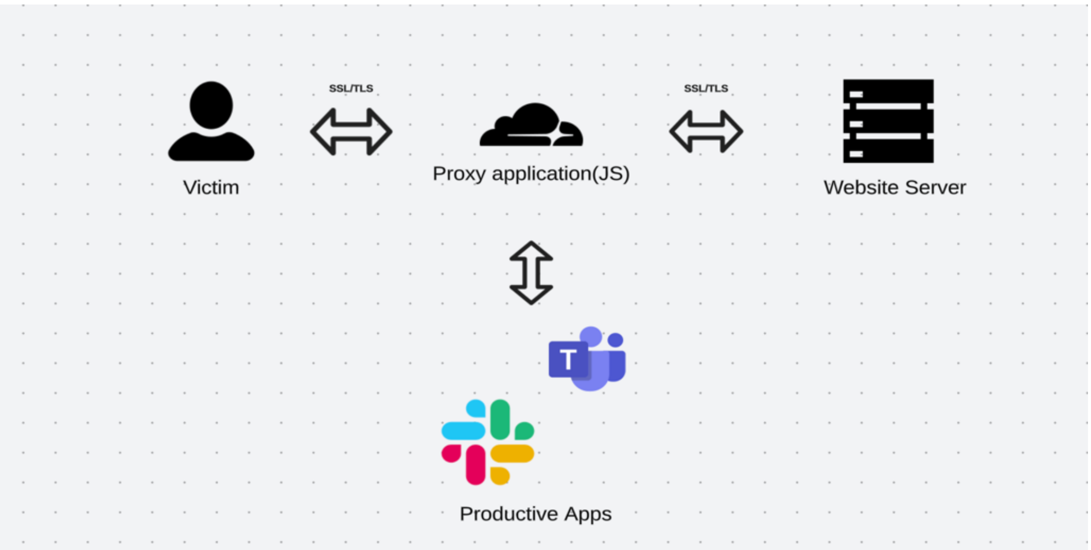


Figure 3 Serverless Architechture

The victim is an individual attempting to log into their account, which might be linked to various services like Office 365, Microsoft Teams, or other enterprise services provided by Microsoft. The victim inputs their login credentials (username and password) into what they believe is a legitimate Microsoft login page. They might be accessing this page via a link received through an email or other communication means, which is actually crafted by the attacker.

Deployed as a serverless function, this JavaScript-based proxy application is hosted on platforms such as AWS Lambda or Azure Functions, making it agile and difficult to trace due to the temporary nature of serverless computing. This proxy intercepts the login request from the victim to login servers. It can capture the credentials submitted by the user and possibly perform actions such as logging these credentials or even modifying the request before forwarding it to the actual server. In a phishing scenario, the primary objective is to steal the victim’s login credentials, and login cookies which can provide access to a wide array of services and sensitive organizational resources.

The Website server the legitimate server that handles authentication requests for accounts. The server receives what it perceives to be legitimate authentication requests from the victim. However, these requests are relayed through the proxy, which means they could be altered or monitored without the server's knowledge. If the server processes these requests without detecting the manipulation, it could unintentionally validate the attacker's access or provide sensitive data in response, such as authentication tokens.

There is an integration of productive applications like Microsoft Teams and Slack. If attackers successfully steal credentials, they can access these applications, potentially leading to further phishing attacks inside an organization and data breaches or other malicious activities.

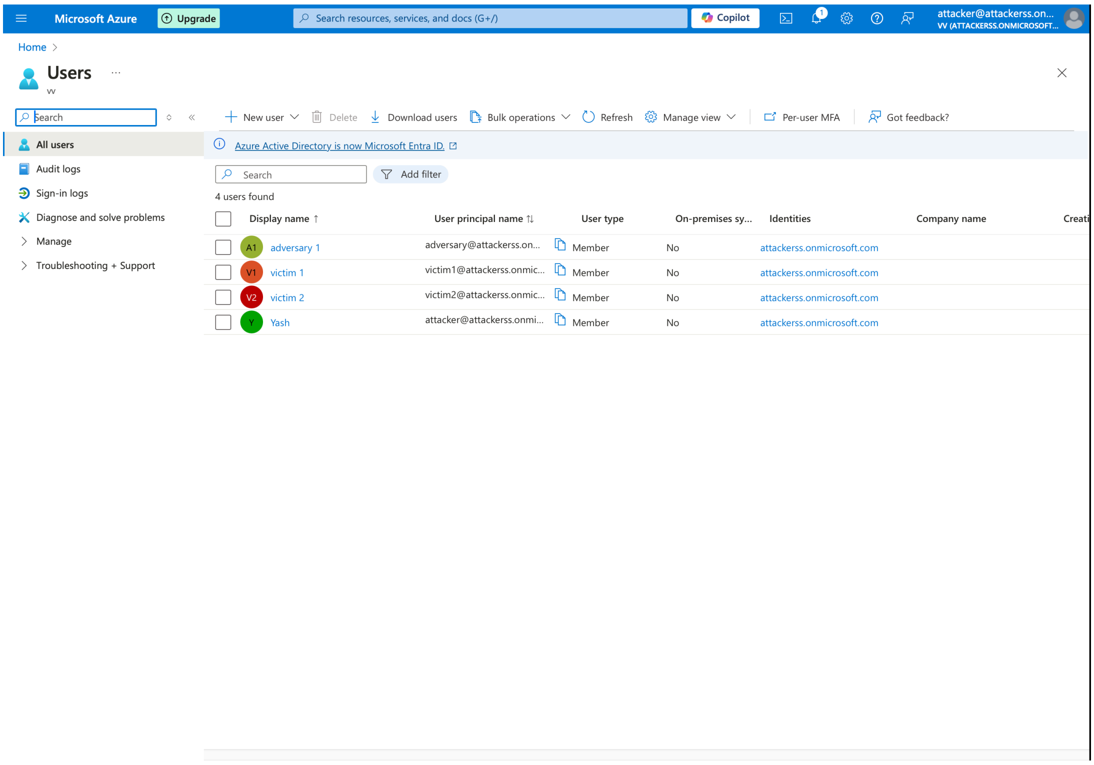
3.6 Flow of Data and Interaction:

The victim sends an HTTP(s)request to the proxy application what they believe is the legitimate login service. This request usually includes very sensitive data like their username, password, and possibly other authentication factors like a one-time password. The request might be sent with an HTML form using the POST method. The request is intercepted by the serverless proxy application. This proxy which is usually implemented using JavaScript in a cloud-based serverless environment (such as AWS Lambda, Google Cloud Functions, or Cloudflare Workers) acts as a man in the middle that will capture all the data sent by the victim. The proxy application will process the intercepted data. For example, In a Node.js environment, , the data might be parsed with middleware called body-parser to extract credentials and other form inputs. The proxy forwards this data later from a temporary storage facility or memory. The proxy program forward the intercepted credentials to the authorised login server. Minimal or no change is done with this forwarding to guarantee the request is handled as a legitimate login attempt.. The proxy might use an HTTP client library (Fetch API) to replicate the victim's original request. Upon successful authentication, the legitimate server responds with a session cookie or token, which is used to maintain the user's session. This token is crucial because it allows the attacker to access the victim's account without re-entering credentials or MFA. The proxy application captures these tokens, often extracting them from the Set-Cookie header in the HTTP response. The proxy application stores the captured credentials and session tokens and sends them to productive applications which alerts whenever new credentials and tokens are received. The TLS is always resolved by the Cloud service. So there is no breakage of any SSL OR TLS

CHAPTER 4

4 Implementation

4.1 For Simulation made a Microsoft business email for 4 User .


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
attacker@attackerss.on...
VV (ATTACKERSS.ONMICROSOFT...
Home >
Users
vv
Search
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Troubleshooting + Support
New user
Delete
Download users
Bulk operations
Refresh
Manage view
Per-user MFA
Got feedback?
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter

4 users found

Display name ↑	User principal name ⇅	User type	On-premises sy...	Identities	Company name	Creati
A1 adversary 1	adversary@attackerss.on...	Member	No	attackerss.onmicrosoft.com		
V1 victim 1	victim1@attackerss.onmic...	Member	No	attackerss.onmicrosoft.com		
V2 victim 2	victim2@attackerss.onmic...	Member	No	attackerss.onmicrosoft.com		
Y Yash	attacker@attackerss.onmi...	Member	No	attackerss.onmicrosoft.com		

Figure 4 Microsoft business email creation for simulation

4.2 Server Based (Using Evilginx)

4.2.1.Domain Name

Registered a domain name with webhost365 : trusthaven.info

Used Digital Ocean for setting up a cloud virtual machine . Added the domain name inside the digital ocean domain tab .Copied the nameservers and replaced it with digitaloceans name server as default.

2.VPS(Virtual Private Server)

For a Cloud virtual machine ,created a droplet ,For logging in copied the IP of the droplet. Used terminal(ssh enabled) to login via command

```
Cmd: ssh root@my ip
```

4.2.2. Installed evilginx in Vps.

Resolved dependencies for Evilginx, like downloading go language and configuring environment variable. Installed requirement packages like git make in the machine .After the packages is installed ,Downloaded the Evilginx files in the machine .After coming in the Evilginx folder use make ,so that it will build the machine.

4.2.3. Domain and Cert for Evilginx:

Created TXT records in my domain as when Evilginx starts more than one subdomains are created. To create TXT, download the certbot on the Linux machine. Created a TXT record using certbot .After copying the TXT record pasted the values inside the TXT record and created it. Along with this, created A records as well. The next step is to create CNAME records in domain because it wont show any error whenever a new subdomain in created in Evilginx

4.2.4.Start Evilginx

Configured IP address and the domain name inside Evilginx.After configuring the domain and IP,made a custom phishlet of o365 for phishing.Then setup the hostname to trusthaven.info and enable the phishlet.The SSL certificates will be successfully enabled .This mean that the phishing page can be used. Then create lures and get the url for phishing .Send the URL to the user by SMS,email,etc.

4.3How Does it Work?

In this attack, an attacker sets up a phishing site that impersonates a legitimate website. When a user thinks they are accessing a legitimate site, they are connecting to the attacker's server. This server uses a self-signed SSL certificate, which can appear valid and secure (displaying a green lock icon) in the user's browser.

This attacker's server doesn’t host any content itself; rather, it acts as a proxy. When the user sends a request, the attacker’s server forwards this to the actual website, establishing a second, distinct TLS connection. In this setup, the attacker manages two encrypted connections: one with the user and another with the legitimate website. The attacker can decrypt the user’s requests using their private key from the self-signed certificate and forward these requests to the legitimate site. Responses from the real site are intercepted by the attacker, who can alter them (e.g., changing URLs to malicious domains) before sending them back to the user. This approach allows the attacker to observe and manipulate all transmitted data in clear text, including sensitive details like login credentials and security tokens. If the site uses two-factor authentication (2FA), such as codes sent via SMS or generated by an app, these can also be captured and exploited by the attacker. Once the user logs in, they unknowingly provide the attacker with a valid session cookie. With this cookie, the attacker can impersonate the user on the legitimate site, performing actions like transactions or accessing sensitive information, all without triggering any security warnings or certificate errors on the user’s end. This makes the attack particularly insidious and effective.

When the user clicks on the link and reaches the server controlled by the attacker doesn’t host anything itself but it takes the user’s request and relays it to the real victim site. Whatever the victim side responds with the HTTP response the attacker server can then rewrite so, for example, he changed domain names to his domain and then forwarded it back to the victim and so effectively have this man in the middle going on between the victim client and the victim server and the attacker has positioned himself in the middle and it's important to understand that the attack would be not trying to break SSL in this process he is not hoping that you know he will use self-signed certificates and the user will click through. The attacker effectively deals with 2 separate TLS sessions so on the left you have one class session that the victim established with a phishing page everything is encrypted. The attacker has an encrypted self-signed certificate. The victim observes this valid certificate for the phishing site so he sees the green lock and thinks that everything is good. The attacker will be able to decrypt the traffic because it is his own key . The attacker is a client towards the second TLS connection on the right and he can just replay the users get requests and post requests to the real victim server right so at the end of the day the attackers have access to everything in clear text and there are no warnings on either side of communication that would indicate that someone is eavesdropping. In this way, credentials are stored in transits and what is even more interesting is that although there is the use of 2FA and MFA where the user will receive an SMS or will open up like an app on their phone and will copy and paste their code from that app this code will also go through the attacker server and so at the end of this process the user has logged in for real on the victim site. He has an authenticated cookie that allows the user to just click through, everything is working but the attacker now is in control not only of the user credentials but also in possession over the authenticated cookie so now the attacker can use that cookie that is authenticated m has passed the 2-factor authentication step perform arbitrary activities on the server in the name of the user

4.4.Serverless Model (Using Cloudflare)

4.4.1Reverse proxy script

Burpsuite: For developing a reverse proxy script and credential and token handling Setup burpsuite and intercepted requests to the original O365 by logging with a credential and inspecting As intercepted traffic. Looked for how identity tokens are transmitted in requests. They were sent over secure channels (HTTPS) and stored securely. Analyzed where tokens are included in requests (e.g., HTTP headers, body). Evaluated the scope and expiration of tokens. Tokens have the least privilege necessary and expire after a short period.

Steps:

1. Phishing Email: Crafted phishing email used to lure users to the fake login page.
2. Cloudflare Workers: This serverless platform is employed to run the JavaScript code that handles the phishing attack. Cloudflare Workers allow for efficient interception and manipulation of HTTP requests in real time.
3. JavaScript: The core programming language used to implement the AiTM attack logic within the Cloudflare Worker.
4. Slack: Used for real-time notification of captured credentials and session cookies.

4.4.2Using Serverless Functions for AiTM Attacks

Phishing Proxy Setup

Phishing Application Deployment: deployed a serverless function to handle HTTP requests. This application is a single file application which is written in JavaScript and its role is to proxy traffic between the user and the original target website. This serverless function intercepts and forwards requests from the user to the original target website. It also captures responses from the target website and relays them back to the user. During this process, the function will log or manipulate sensitive data like authentication cookies or credentials.

4.4.3Intercepting Capturing and Using Session Cookies:

The proxy application (serverless function) intercepts and captures session cookies and other sensitive information as it processes the user's requests and responses. This allows attackers to steal the session tokens from the authenticated sessions. Once the attacker has obtained a session cookie he will be able to inject it into the browser or a separate session which will lead to effectively impersonate the victim(user) and gaining unauthorized access.

4.4.4 Integration of Productive Application

Productivity applications like Slack and Microsoft Teams are used in AiTM attacks to increase the attack's effectiveness. Slack will be configured to send real-time alerts or notifications. Once an attacker's serverless function captures sensitive data (e.g., credentials or session cookies), it can immediately transmit this information to a Slack channel These apps offer a simple interface for attackers to access and review the captured data. Integration with APIs allows for seamless data transfer without manual intervention.

Serverless functions or other automated tools can be set up to interact with productivity apps. For instance, automated messages or alerts can be sent to Slack or Teams channels when specific events occur, such as when a new session cookie is captured. Slack supports incoming webhooks that can be used to send data. Attackers can use these webhooks to automate the process of sending captured data to their communication channels.

4.5 The Reverse Proxy Script:

Initial Configuration

Key variables:

1. upstream, upstream_path: is used to specify the destination server where all requests should be forwarded.
2. https: makes sure whether to use HTTPS or HTTP for forwarding requests
3. webhook: URL of a Slack webhook used for sending alerts about specific events detected by the script.
4. blocked_region, blocked_ip_address: Arrays that list regions and IP addresses from which access should be denied, used for restricting the IP's based on region

Event Listener

The script listens for the fetch event, which is initiated every time a request comes to the Cloudflare Worker. The event handler represents to the fetchAndApply function to process every request.

Function: fetchAndApply

This function is the main fuction of the app which handles request modify them, captures sensitive information and repospondes.

Request Analysis

1. **Extract Region and IP**: It extracts the geographical region and IP address from the request headers.Which helps in blocking some IP basis on region.
2. **Modify Request URL**: On the basis of configuration this alters the protocol and constructs a new URL which will point to the upstream server. This will make sure that the request looks like it came from a original website.

Security Controls

1. **Block List Enforcement**: Before going ahead it will check if the request (IP or region)is coming from the region the region that is on a block list. If it does then it will immediately return a 403 (Forbidden) response which will help stop the request.

2. **Credential Capture**: For POST requests, the app analyzes the body to extract login credentials. This is will capture sensitive information like logging in usernames and passwords. This kind of data is formatted into an HTML message and sent to Slack, which will be used for further purpose of loohing in and malicious activity

Forwarding and Response Handling

1.Forwarding the Request: It sets appropriate headers and forwards the request to the upstream server.

2.Handling WebSockets: If the original request upgrades to a WebSocket . It will maintain this upgrade in the forwarded request which will make sure the functionality like real-time updates works without stopping.

3.Response Modification: After getting the response from the upstream server the app modifies headers to remove security policies that might interfere with the client-side rendering. It also modifies cookies to reflect the proxy's domain instead of the upstream server's domain, managing session continuity securely.

Helper Functions

replace_response_text

- This function rewrites content in the response, replacing all references to the upstream domain with the proxy's domain. This step ensures that any embedded links or references do not expose the use of the proxy.

slack

- Sends formatted messages to a Slack channel using a webhook. It is used to handle communication failures by catching exceptions and logging errorsif the sensitive information isnot captured.

CHAPTER 5

5 Mitigation

5.1Phish-Resistant MFA Solutions

5.1.1 FIDO (Fast Identity Online)

FIDO is designed to be resistant to phishing attacks due to its use of public key cryptography. During the registration process with a service, the user’s device creates a new public-private key pair. The public key is registered with the online service, but the private key remains securely stored on the user’s device and never leaves it.The user must prove their presence through a secure action on their device, such as pressing a button on a hardware token (like a YubiKey) or using a biometric sensor.Authentication happens locally on the device, not through a remote server or an interactive process susceptible to interception. This means that even if a phisher redirects a user to a fake site, they cannot access or use the private key; they would need the physical device itself.

5.1.2Certificate-Based Authentication

Similar to FIDO, certificate-based authentication uses digital certificates to verify a user's identity. The certificate contains a user’s identity information and a public key, issued by a trusted Certificate Authority (CA).Certificates facilitate encrypted communications and digital signatures, making sure that even if data is intercepted, it cannot be decrypted without the corresponding private key. Unlike traditional password-based systems, certificates do not rely on reusable credentials that can be phished or intercepted.

5.1.3 Conditional Access Policies

Conditional Access policies add an additional layer of security by assessing the context of a login attempt before granting access: Conditional Access systems evaluate the risk level of the user and device attempting to access the resource. This assessment can include checks for device compliance, location, IP reputation, and whether the device is marked as secure. Based on the risk assessment, access to resources is granted or blocked dynamically. For example if the some user in seen logging in from a different location then which he usuauall doesn’t then additional authentication will be required to further log in

CHAPTER 6

6 Discussion

Table 1 Comparison of Sever-based and Serverless Infrastructures

Aspect	Server-Based AiTM Attack	Serverless AiTM Attack
Infrastructure	Requires a dedicated server (e.g., VPS)	Utilizes cloud functions (e.g., Cloudflare Workers)
Scalability	Owned domains	Have a lot of cloud domains
Certificates	Mostly Manual Certificate	Cloud Services provides certificate support
Deployment Complexity	Requires manual setup and configuration (e.g., Evilginx)	Easier to deploy with minimal setup using serverless platforms
Cost	Fixed costs related to server maintenance	Pay-as-you-go model, lower cost for low traffic
Detection	Easier to detect due to fixed IP addresses and known server patterns	Harder to detect
Example Tools	Evilginx, Modlishka	Cloudflare Workers, AWS Lambda

6.1Comparision of infrastructure

In terms of infrastructure : server-based AiTM attacks require attackers to set up and maintain a dedicated server, such as a Virtual Private Server (VPS). The setup will require continuous maintenance but serverless Aitm works on third-party cloud functions like Cloudflare Workers etc. This allows the attacker to run the code on the cloud environment and need not need to invest in servers' whole maintenance. Server based attacks depend on owned domains or rented domains which means the resources are limited. Whereas serverless attacks have. The no of domains as the service is provided by organizations like Cloudflare and AWS.So serverless method has more resources.

In terms of Certificates: The server-based method requires to manually handling SSL/TLS certificates which is a bit harder and takes time and also cannot be that good as browsers might find out that the certificate is a makeshift. The serverless method of certificate management is done by a third party or the service providers. This makes it look more genuine and easy. While deploying the server-based method the person needs technical skills in order to set it up properly because the task is complex while setting up and configuring servers and tools like Evilginx..The serverless method is comparatively very simple to deploy as it involves minimal setup and allows attackers to launch malicious functions quickly using platforms which are easy to use

Server-based methods have fixed costs which is related to the maintenance of the server, which can be expensive even no matter what is the scale of the attack. Serverless attacks have the advantage of you pay as you use which makes it cost effective specifically when we don't know the rate of traffic which is sometimes unpredictable. When it comes to detection server based method uses a fixed IP and can be detected comparatively easily. Serverless methods can be challenging to detect because they depend on decentralised and temporary cloud computing which does not stick to static infrastructure.

6.2 Mitigation and its effectiveness

Table 2 Mitigations and Deatails

Phish-Resistant MFA Solutions		**Details**
FIDO2 Security Keys	Yes	Strong protection due to hardware-based authentication resistant to phishing attacks in both server-based and serverless environments.
Windows Hello for Business	Yes	Tied to TPM, making it resistant to phishing and capable of preventing token theft in both environments.
Certificate-Based Authentication	Yes	Uses certificates, providing strong protection by ensuring only authorized devices can authenticate in both server-based and serverless scenarios.
Password less Phone Sign-In	No	Vulnerable to AiTM attacks; tokens can be intercepted even without a password in both server-based and serverless environments.
Phone Number and SMS	No	Susceptible to interception and social engineering attacks; not protected against AiTM in either environment.
Username and Password	No	Weakest form of authentication; easily phished and vulnerable without additional layers like Conditional Access in both environments.

Table 3 Authencation Methods and efffect

Authentication Method	**Mitigation**
Phone-call	No
Microsoft Authentication App and Number matching and additional context	No
Auth App(Microsoft)	No
Auth App and Number match (Microsoft)	No
Auth App and Additional context)	No
SMS	No

Table 4 Conditional access policies and impact

Policies		**Details**
Require Device Compliance	Yes	Ensures that only compliant devices can access resources, reducing the risk of token theft via AiTM attacks in both environments.
Conditional Access Trusted Locations	Yes	Restricts access to specific IP ranges, protecting against external AiTM attacks in both environments.
Require Hybrid Azure AD Joined Devices	Yes	Limits access to devices that are part of the organization's directory, reducing exposure to AiTM in both server-based and serverless contexts.
Entra Global Secure Access	No	Provides enhanced security by controlling access through verified and compliant channels, helping to mitigate AiTM risks in both server-based and serverless contexts.
Continuous Access Evaluation (CAE)	No	Removes access based on user condition changes but doesn’t protect against initial AiTM token theft in either scenario in real time
Conditional Access Session Controls	No	Limits the session time window but doesn’t prevent token theft during the session in either environment.

6.3 Uses and Misuses of Phishing Infrastructure

How can the use of Server-based and serverless infrastructure help in phishing assessments and employee training to reduce and prevent AiTm threats?-

In cyber security, organizations form teams of security professionals called as ”Red team” and “Blue team” The Red team act as attackers. They would design and implement realistic attacks to test the ability of the blue team to defend against different attack situations. These simulations will test the defences of the organizations by using the techniques that real-world attackers might use. For Example, sending fraudulent emails that might trick the employees to click on malicious links and reveal sensitive information.

The Blue team is always focused on the defensive side of the organization. Their task will be to monitor and respond to attacks launched by the Red Team. For example, if the red team makes a phishing attempt, it's the role of the blue team to detect, respond, mitigate and report it. Also, the blue team is responsible for isolating affected systems and conducting analysis.

Both teams are an important part of an organization who wish to protect its digital assets. Phishing assessments are conducted in organizations to make employees aware and stay up to date with the trending attacks.

Real Attack Simulations: By using both server-based and serverless infrastructures and organizations can make a very realistic phishing situation that will resemble the techniques tactics and procedures (TTPs)used by real-world attackers This will help make sure the training programs are effective. This will make sure that the employees are always ready how to react towards advanced phishing attacks if they encounter. Server-based infrastructure is useful for creating detailed and controlled environments that are similar to the organization's actual network setup, which will show more realistic attack simulation. Similarly, serverless infrastructures are useful in rapidly modifying and adapting to different situations and new threats This will help the employees to not only stay trained for current situations but also up-to-date attack situations that attackers might use.

Prevention of getting used to phishing methods : Employees can become used to repeated phishing exercises. Both server-based and serverless infrastructures allow for regular modification of phishlets so that it doesn't get repetitive. Specially serverless method. This continuous refreshment keeps the training engaging and challenging, ensuring that employees remain attentive. Dedicated servers also make sure that necessary resources are made available to implement a large-scale phishing operation without any performance issues. But the drawback here is the server-based setups can increase visibility due to their IP which depends on static addresses. This makes it easier to find and block the blue team. Also maintaining physical and virtual servers costs high charges which makes it expensive to run and manage

Case 1: Normal Phishing Assessment: In a typical phishing assessment, a server-based infrastructure provides an advantage because of its control over the server and its modification. This infrastructure can install and use different software and configurations specifically used for a complex phishing attack scenario Dedicated servers also make sure that necessary resources are made available to implement a large-scale phishing operation without any performance issues. But the drawback here is the server-based setups can increase visibility due to their IP which depends on static addresses. This makes it easier to find and block the blue team. Also maintaining physical and virtual servers costs high charges which makes it expensive to run and manage

On the contrary serverless infrastructure is highly beneficial in situations where scalability and cost efficiency are top priorities. The serverless model dynamically allocates resources based on demand, which is especially useful for handling varying loads during phishing assessments. Its pay-as-you-go pricing model minimizes overhead costs, making it more cost-effective, particularly for assessments with fluctuating traffic. The temporary nature of serverless functions, operating from different IP addresses, also reduces the risk of detection, as these functions don't maintain a constant presence that can be easily flagged. However, serverless infrastructures have limitations, particularly in terms of control over the runtime environment, and potential delays during cold starts—when the function is initiated—can impact the speed and flexibility required in certain phishing campaigns.

Case 2: When Blue Team Has Identified the Server in Server-Based Attacks : If the Blue Team has already detected a server-based attack, the visibility of the infrastructure becomes its biggest weakness. Once a server is identified, it can quickly be blocked or closely monitored, which greatly reduces its effectiveness for ongoing phishing operations. This visibility limits the usefulness of the server-based setup for further attacks. However, if the server goes unnoticed, it can still be used to carry out more complex and longer-lasting phishing attempts by continuously adjusting its methods as the situation evolves. This is the flexibility that allows attackers to maintain their operations

However, serverless infrastructure has the big advantage of being much harder to detect. The temporary and dynamic nature of serverless functions make it difficult for the blue teams to predict or react which allows the phishing campaigns to continue from different locations and IP addresses. Also, serverless infrastructure can be taken down and redeployed. This makes sure that the attacker can adapt the strategies and bypass defences that are previously identified. This makes serverless infrastructure more effective for dynamic phishing situations where fast modification is important. However serverless infrastructure has limitations. When it comes to handling larger or complex phishing campaigns because it involves third-party services.

Both server-based and serverless infrastructures offer different kinds of advantages. But they also come with their challenges when applied to phishing operations. The choice to choose between them should depend on the specific objectives of the phishing activity. The technical skills and strength of the blue team should also be considered. The strategy also is an important aspect. Server-based environments are better for a controlled and detailed operation. But they are more vulnerable to detection and blocking or shutdown. Serverless approaches offer flexibility and are cost-effective and also sleath making them ideal for avoiding detection and quickly adjusting to the defences

6.4 Misuses of infrastructures

The misuse of server-based and serverless infrastructures designed for assessments poses a critical threat. We can say the dual-use nature of the technologies. The tools and techniques created to improve security through controlled phishing simulations can be used differently. It can be used for malicious purposes if they fall into the wrong hands. Both infrastructures are capable of launching a complex phishing attack. So there is also a need to use this infrastructure with strict security policies and protocols. This is a real danger that these infrastructures could be exploited to conduct malicious activities. It can lead to more complex cyberattacks like BEC, Malware delivery, stealing of personal data and other malicious operations resulting in financial and other kinds of loss

Also, the risk is multiplied in situations in which security measures are weak or can be easily bypassed. Both server-based and serverless infrastructures are vulnerable to hijacking by malicious actors out of the organization. Once Compromised the attackers could use the infrastructures to initiate data big data breaches and also expose sensitive personal and organisational information. The consequences are serious like financial loss, damage to reputations and legal challenges that can affect the entities. This why it is important to make sure that the infrastructures are not misused and are always protected against unauthorizes access and data breached.

6.4 Impact of Misuse of Phishing Infrastructures

Financial Losses:The most immediate and major impact of misuse of phishing infrastructure is financial loss. Not only organizations but normal user face direct losses from fraudulent transactions due to phishing's indirect cost including remediation efforts, legal fees and penalties related to data breaches. For normal users, phishing scams might result in the stealing of financial and personal information, which can not only damage their current balance but might affect them in the long term

Reputational Damage:In :the aspects of reputation, people knowing that a business is related or compromised due to phishing attacks cause severe reputational harm. Trust is the most important thing to maintain customer relationships This is what is lost. The damage extends to all the other parties connected to the business like business partners, suppliers and sometimes the whole industry This results in a loss of reputation and casts doubt on security practices

Operational Disruption:Phishing attacks usually aim to target organizational networks. This gives the freedom for deployment of malware, ransomware and other malicious activities. This leads to operational disruptions which includes system outages, data loss and interruption of essential services. The downtime not only incurs financial costs but also productivity and delays the service delivery. Potentially harming the organizations market standing and competitive advantage

Legal and Regulatory Consequences – Strict regulations to protect consumer data and a failure to secure this data due to phishing infrastructure misuse can lead to serious legal and regulatory consequences which is enforced by many jurisdictions. Compromised infrastructures which results in breaches can put the organization in violation of data protection laws like the GDPR in the Europe and HIPPA in the U.S.A which will also lead to fines, sanctions and legal battles and indirectly lead to financial, reputational damage to the entities involved in both short and long term

Loss of Trust in Digital Communications :On a large scale. The increase in misuse of phishing infrastructure will lead to scams. This will negatively affect the trust users have in digital communication. As phishing attack become more frequent, users and organisations will become very cautious which will slow down the adoption of new technologies ..These entities will always hesitate to interact with legitimate services as differentiating between real and fake communications becomes very difficult which will result is a loss of trust in digital platforms.

Strengthening of Criminal Networks :The successful exploitation of phishing infrastructures will not only results in financial losses for victims but also help criminal networks to become strong. The profits gained through these malicious activities can be reinvested to make the phishing techniques even more sophisticated and increase the scale of operation. This will make it even harder to detect and for cybersecurity professionals to fight against. This will continue the improvement of criminal operations and enables criminals to launch more complex and largescale attacks across the global networks

CHAPTER 7

7 Conclusion

A thorough analysis of Adversary in the Middle Attack (AiTM) phishing attack is provided in the research. It is mainly focused on both server-based and serverless models, including their implementation, working and examining the various defense and mitigation techniques. The findings show that there is a need for robust and multilayer security strategies due to the evolving threat of phishing. It was found out that the significant operational difference between server-based and serverless AitM attacks includes variation in scalability and detection challenges which is a key finding. Server-based attacks allow for more control and customization but they also require more infrastructure management. They are easier to detect due to their static nature. On the other hand, serverless attacks use cloud functions that make them more cost-effective sleath, and challenging for cybersecurity defences in some scenario

One more important finding was that AiTM attacks bypass traditional Multi-Factor Authentication (MFA). The attack can intercept and relay authentication processes in real-time. It captures both login credentials and session tokens or cookies bypassing some of the complex MFA. The project highlights the urgent need for more secure and advanced phish-resistant authentication solutions. One more finding is that there is no single proper defence mechanism that will provide total protection against AiTM attacks. Only some combination of MFA. certificate-based authentication and conditional access policies can reduce the risks. FIDO security keys and Windows Hello for Business were highly effective. Due to hardware-based authentication which is resistant to interception and replay attacks. But is not always possible to carry and implement hardware everywhere. Certificate-based authentication also provides a strong defense which makes sure that only authorized devices can get access which reduces the attack surface

However, the project also examines different and widely used methods for authentications like SMS-based verification and standard username/password combinations which stay vulnerable and should be replaced with other secure alternatives. Conditional access policies like: as requiring device compliance which restricts access to trusted locations, and hybrid Azure AD-joined devices offer a layer of security but can be degraded down. But it makes it harder for less skilled attackers to use stolen tokens or credentials to gain unauthorized access

.

The project also highlights the importance of continuous security awareness training and phishing assessments. Using both server-based and server-less infrastructure to simulate a phishing operation. Provides organizations with a flexible and very realistic environment for phishing assessment and training. This helps employees to engage with a wide range of phishing scenarios which enhances their ability to recognize and responds to real threats in future. The study also points out the risk of misusing the phishing assessment infrastructures.If not properly managed and secured can be exploited for malicious activities.

In conclusion ,though AiTM phshing attacks are evolving and major threat to organizational security the use of a ~~comprehensive defense strategies including advanced authentication methods, conditional~~ access policies and security training will offer string protection. There is a need for the organization to regularly review and update security protocols to counter the evolving threats. Future research should focus of improving the detection method fo the serverless AiTM attack. Also Exploring the use of AI and machine learning in real-time phishing detection and mitigation. Studying the long-term effectiveness of phish resistant MFA solutions in different scenarios can be also explored. Also investigating the psychological factors that contribute to phishing and developing more effective user education can play a important role in reduction of human vulnerabilities in phishing attacks.As phishing evolves organizations and users must adopt secure and multifaced approach to cybersecurity to protect the digital assets and maintain trust

Bibliography

1. AiTM phishing attacks on the rise | SC Media (n.d.). Available at: https://www.scmagazine.com/brief/aitm-phishing-attacks-on-the-rise (Accessed: 14 September 2024).

2. AiTM Phishing Attacks: Stolen Session Cookie Creates Havoc in Financial Organizations (n.d.). Available at: https://www.linkedin.com/pulse/aitm-phishing-attacks-stolen-session-cookie-creates-havoc-financial/ (Accessed: 14 September 2024).

3. BEC Attacks in 2023: What Organizations Need to Know (n.d.). Available at: https://www.bitdefender.co.uk/blog/businessinsights/bec-attacks-in-2023-what-organizations-need-to-know/ (Accessed: 14 September 2024).

4. Chanti, S. and Chithralekha, T. (n.d.) A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration, 9 (89): 2394–7454. doi:10.19101/IJATEE.2021.875031.

5. Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog (n.d.). Available at: https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/ (Accessed: 14 September 2024a).

6. Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog (n.d.). Available at: https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/ (Accessed: 14 September 2024b).

7. Evilginx 2 - Next Generation of Phishing 2FA Tokens (n.d.). Available at: https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/ (Accessed: 14 September 2024).

8. How attackers can bypass MFA using AiTM, and how to defend against it | Claranet UK (n.d.). Available at: https://www.claranet.com/uk/blog/how-attackers-can-bypass-mfa-using-aitm-and-how-defend-against-it (Accessed: 14 September 2024).

9. Identifying Adversary-in-the-Middle (AiTM) Phishing Attacks through 3rd-Party Network Detection - Microsoft Community Hub (n.d.). Available at: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/identifying-adversary-in-the-middle-aitm-phishing-attacks/ba-p/3991358 (Accessed: 14 September 2024a).

10. Identifying Adversary-in-the-Middle (AiTM) Phishing Attacks through 3rd-Party Network Detection - Microsoft Community Hub (n.d.). Available at: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/identifying-adversary-in-the-middle-aitm-phishing-attacks/ba-p/3991358 (Accessed: 14 September 2024b).

11. Introducing the Amazon Linux 2023 runtime for AWS Lambda | AWS Compute Blog (n.d.). Available at: https://aws.amazon.com/blogs/compute/introducing-the-amazon-linux-2023-runtime-for-aws-lambda/ (Accessed: 14 September 2024).

12. Rising AiTM phishing attacks: how to protect against them | Chorus (n.d.). Available at: https://www.chorus.co.uk/resources/rising-aitm-phishing-attacks-what-are-they-and-how-to-protect-against-them/ (Accessed: 14 September 2024).

13. Safi, A. and Singh, S. (2023a) A systematic literature review on phishing website detection techniques. Journal of King Saud University - Computer and Information Sciences, 35 (2): 590–611. doi:10.1016/J.JKSUCI.2023.01.004.

14. Safi, A. and Singh, S. (2023b) A systematic literature review on phishing website detection techniques. Journal of King Saud University - Computer and Information Sciences, 35 (2): 590–611. doi:10.1016/J.JKSUCI.2023.01.004.

15. Shaikh, A.N., Shabut, A.M. and Hossain, M.A. (2016) A literature review on phishing crime, prevention review and investigation of gaps. SKIMA 2016 - 2016 10th International Conference on Software, Knowledge, Information Management and Applications, pp. 9–15. doi:10.1109/SKIMA.2016.7916190.

16. THE EVOLUTION (1997).

17. The Weaponization Of AI: The New Breeding Ground For BEC Attacks (n.d.). Available at: https://www.forbes.com/councils/forbestechcouncil/2024/06/14/the-weaponization-of-ai-the-new-breeding-ground-for-bec-attacks/ (Accessed: 14 September 2024).

Appendix

1. GITLAB address : https://git.cs.bham.ac.uk/yxn357/implementation-of-phishing-attack-and-defending-against-them
2. Video of attack implementation is also uploaded on git lab
3. Custom Phishlet for O365 login on gitlab
4. Reverse Proxy script on gitlab
5. https://bham-my.sharepoint.com/personal/yxn357_student_bham_ac_uk/_layouts/15/guestaccess.aspx?share=ErZmZeLw8XNMg-U3As0YSMQBKV8QF6FRI9Ro6_g4WOn3Qg&e=QfxlR9 (has the sever based attack implementation video)