CWL
CyberWarFare Labs

DETECTION STRATEGIES FOR

APT CLOUD INITIAL ACCESS

WWW.CYBERWARFARE.LIVE

ABOUT OUR

CYBERWARFARE LABS

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

About Speaker

Harisuthan S

Senior Security Engineer

He Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defense. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks.

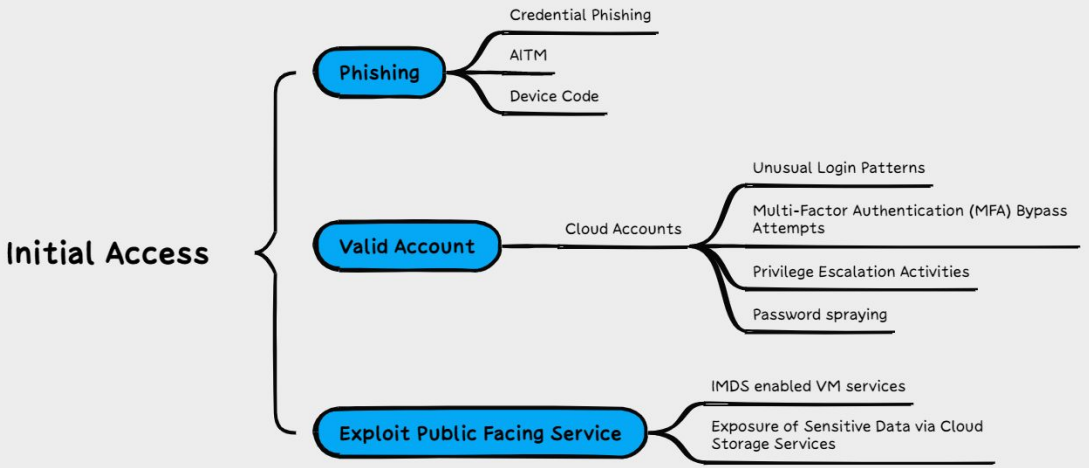
Table Of Content

MITRE ATTACK
CLOUD MATRIX

CLOUD

INITIAL ACCESS

Adversarial tactics and techniques used to gain an initial foothold in cloud infrastructure



CREDENTIAL

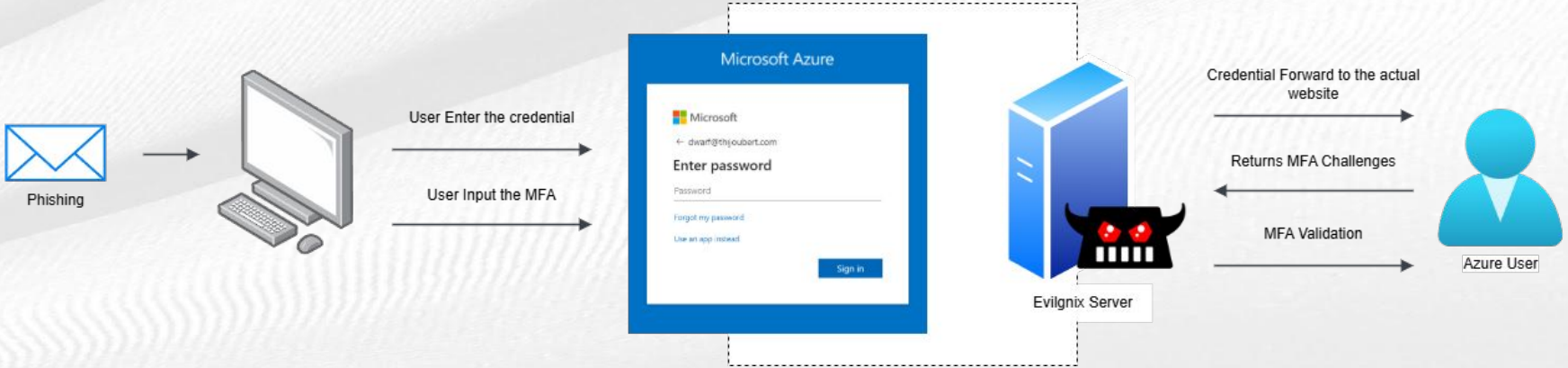
PHISHING

Credential phishing is a common initial access technique in cloud environments, where attackers trick users into revealing login credentials through deceptive emails, fake login portals, or social engineering.

Once credentials are obtained, threat actors can access cloud resources, bypass security controls, and establish persistence, often without triggering immediate alerts.

AITM

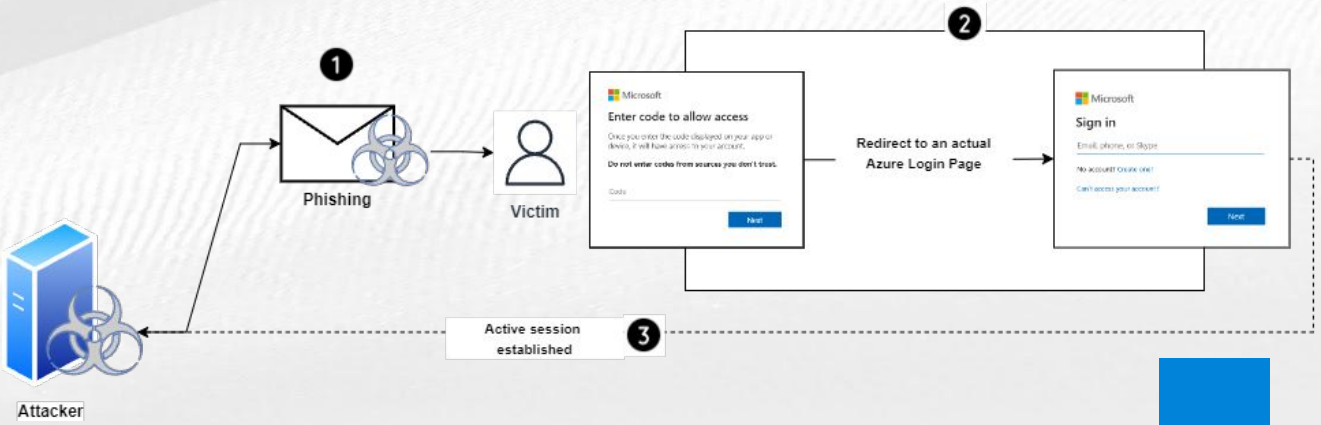
AITM (Adversary-in-the-Middle) is a sophisticated phishing technique where the attacker intercepts and relays communication between a user and a legitimate service—usually during login—to steal credentials and session cookies in real time.



DEVICE CODE

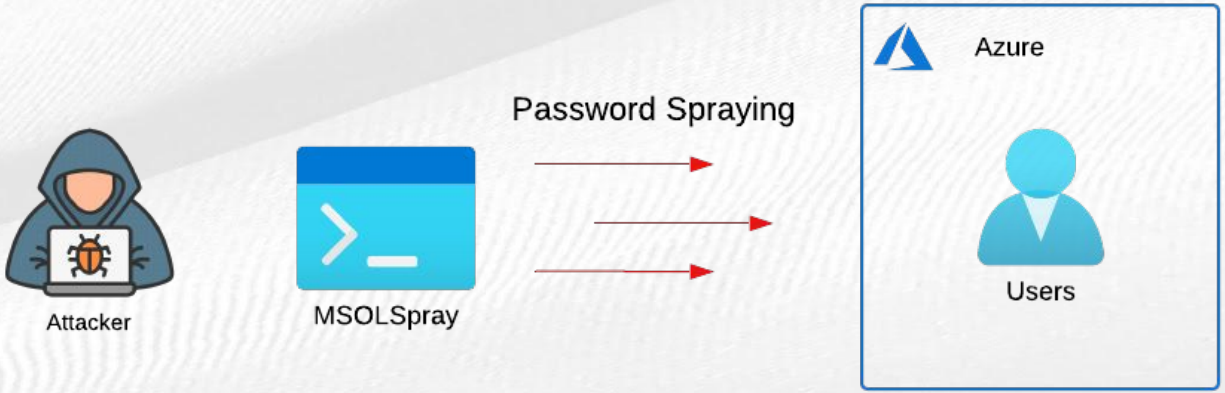
Device Code Phishing is a social engineering technique that targets OAuth-based authentication flows, particularly the Device Authorization Grant

This attack tricks users into approving attacker-controlled applications, granting access to their cloud accounts without ever stealing a password or MFA token.



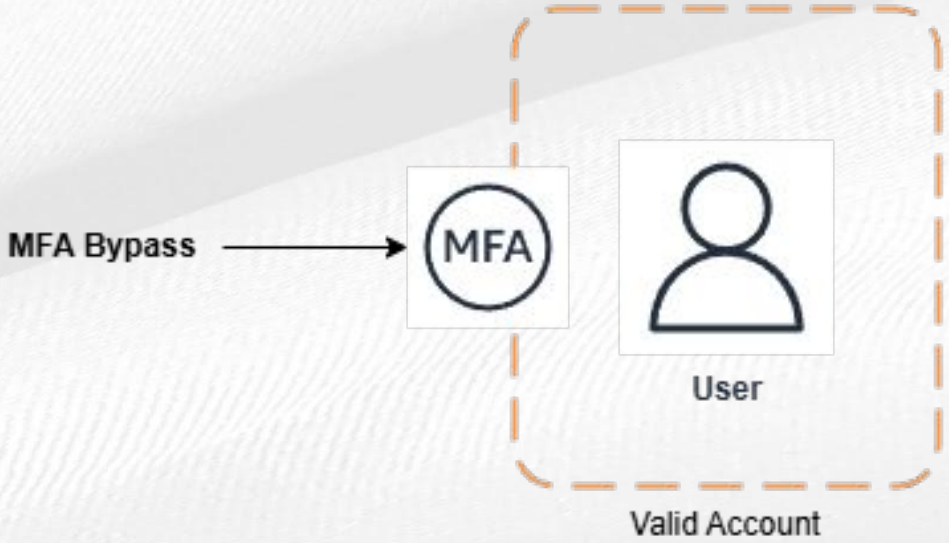
PASSWORD SPRAYING

Password spraying is a brute-force attack technique in which an attacker attempts to gain unauthorized access to multiple user accounts by trying a few commonly used passwords across many usernames.

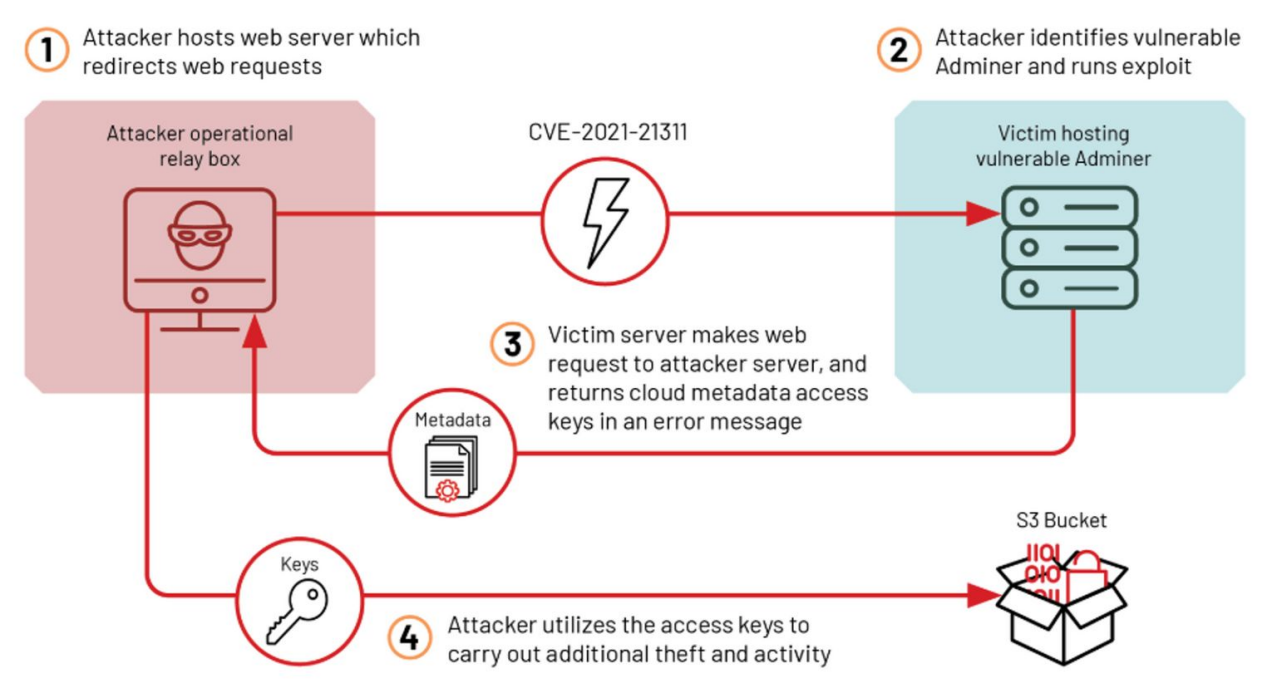


MFA BYPASS

MFA Bypass refers to techniques used by attackers to circumvent Multi-Factor Authentication (MFA) protections, gaining unauthorized access to systems or cloud services despite additional authentication layers being in place.



IMDS ENABLED VM SERVICES



DETECTION STRATEGIES FOR APT CLOUD INITIAL ACCESS

EMULATING “STAR BLIZZARD”: MFA BYPASS VIA ADVERSARY-IN-THE-MIDDLE (AITM)

objective is to emulate the activities of a sophisticated Russian-based threat actor, Star Blizzard, known for targeting academia, governments, and NGOs across the UK, USA, and NATO-affiliated entities.

This simulation involves replicating their advanced Multi-Factor Authentication (MFA) bypass techniques, specifically focusing on Microsoft's Azure Identity Provider (IdP).

CRYPTO EXCHANGE HEIST: BY LAZARUS GROUP (DPRK)

Simulate the Crypto Hack, a real-world-inspired attack where threat actors infiltrated cloud infrastructure to modify legitimate code and drain crypto assets.

THANK YOU

WWW.CYBERWARFARE.LIVE