A Technical Review of the Team filtration Campaign

Aflah[1], Dr Priya P Sajan[2]
[1]*Member, UG Student Computer Science and Engineering (Cyber Security), Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology*
[2]*Member, Senior Project Engineer, C-DAC Technopark, Thiruvananthapuram*

***Abstract*—Team Filtration was a cyber threat campaign that targeted over 80,000 Microsoft Entra ID accounts globally. It is a comprehensive, cross-platform framework specifically built for post-exploitation activities within Microsoft 365 and Microsoft Entra ID. This case study examines the UNK Sneaky Strike cyberattack campaign, which weaponized a legitimate open- source penetration testing tool, detailing how it was used and discussing prevention tactics.**

***Index Terms*—Team filtration, Microsoft Entra Id, Microsoft 365, Cyber threat.**

I. INTRODUCTION

Team Filtration is a powerful post-exploitation and re- connaissance tool primarily targeting Microsoft 365 and Active Directory environments. Originally designed for red team operations and penetration testing, the tool has also been co-opted by malicious actors in campaigns such as UNK Sneaky Strike, where it was used for account takeover, credential harvesting, data exfiltration, and privilege escalation. At the center of this operation was a weaponized variant of the open-source Team Filtration tool, originally designed for red-team reconnaissance in Microsoft 365 environments. At-tackers significantly modified the tool to support initial access, automated credential abuse, advanced persistence mechanisms, and stealth data exfiltration, transforming it into a full-fledged cloud exploitation framework. This report outlines the attack lifecycle, tool modifications, and prevention strategies. Team-Filtration tool was created by Melvin Langvik (Flangvik) he is a c Azure Developer who became hacker, working on targeted operation for Trustedsec organization. The core Purpose and Attack Flow is in three-phase Methodology against Microsoft office 365 environment Enumeration, spraying, and exfiltra- tion. Team filtration is designed to facilitate these stages. This was the original use of team filtration tool and due to this fundamental set of capabilities that malicious actors leverage when weaponizing the tool. The UNK Sneaky Strike campaign is a notable and widespread cyberattack operation primarily aimed at Account Takeover (ATO). It is significant because it weaponizes a legitimate, open-source penetration testing tool called Team Filtration to compromise user accounts within Microsoft Entra ID (formerly Azure Active Directory) and Microsoft 365 environments.

II. METHODOLOGY

This methodology is divided into three primary phases:
Enumeration, Spraying, and Exfiltration
a. Enumeration Phase

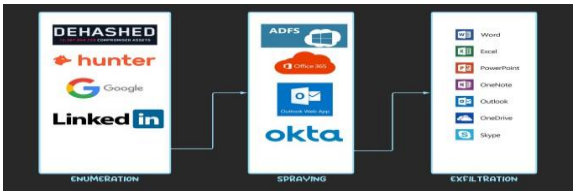

Fig. 1: Method Workflow

This initial phase is about intelligently discovering valid user accounts within the target organization's Microsoft 365 tenant. Instead of blindly guessing, Team filtration focuses on confirming which email addresses or usernames exist, making subsequent attacks far more efficient. Its objective is to compile a list of valid target username or email addresses or any other credential which could be used for enumeration. It uses Dehashed Database accessing large database of pre- viously compromised credentials to identify email addresses associated with the target domain. Google LinkedIn: Utilizing search engines and professional social networking

sites to find employee names, job titles, and often, their corporate email addresses or patterns.

Microsoft Team API Validation: This is the method used by the Team filtration tool. this is one of the most effective and fast method, the tool abuses the legitimate Microsoft Teams API normally through sacrificial Microsoft 365 account controlled by the attacker is used for this method. By sending queries to the API that mimic how a legitimate Teams client would search for or verify a user's presence, the tool can infer whether a given username or email address is valid within the target Entra ID tenant. The API might return different error codes or responses for existing versus non-existent users, revealing the validity of the account. This method is crucial for efficiently building accurate target lists. The outcome should be a refined list that can used for password spraying.

b. Spraying phase After getting list of valid users the Team filtration moves to the next phase that is Password Spraying (Trying to gain unauthorized access to valid user account). Objective of spraying is to gain unauthorized access to valid user accounts by guessing common or likely pass- words without triggering account lockouts. Password Spraying is technique were Instead of trying many passwords against one account password spraying tries a small set of common passwords. against many different accounts. This approach aims to fly under the radar of lockout therefore each only receives a few incorrect passwords attempts before the tool move on. The tool can directly target Microsoft Office 365 authentication endpoints, or federated identity providers like ADFS (Active Directory Federation Services) or Okta, if the target organization uses them for SSO to M365. In TeamFil- tration they use AWS (Amazon Web services) with help of AWS the attacker can evade detection by locating in various geographical regions. And bypass IP-based limiting Security systems often block IPs with too many failed login attempts. Using many different AWS IPs makes it difficult for target organizations to block the attack based solely on source IP. With use of AWS the attackers can avoid Circumvent Geo- Restriction in many organizations block access from unusual geographical locations. Distributed AWS infrastructure allows attackers to launch attacks from locations that might be consid- ered legitimate or less suspicious for the target. If the attacker succeeds in spraying with successful login credential and crucially, Access Token and Refresh Token for a compromised account.

c. Exfiltration Phase Once an account is compromised, Team filtration focuses on maximizing the value of that access by extracting sensitive data and establishing persistent access. The objective is to steal sensitive data from cloud services and ensure continued un authorized access and with the tool the attacker can take the compromised account's access token to systematically extract data from various Microsoft 365 services. With the help of this the attacker will exfiltrate file stored in the user's personal OneDrive, as well as shared document within the SharePoint sites that the user has access to. This could mean that user's entire personal OneDrive can be accessed by the attacker. The attacker can access chat logs, shared attachments within conversations, and contact lists and with getting access Microsoft Graph API they can discover a wealth of information about the organization with this the attacker can gather information about overall Microsoft 365 tenant (Domain name, tenant id) and, they can access user details which is highly sensitive and valuable for an attacker. Persistence Techniques: This can be done by abusing Refresh Token this is a critical persistence method. Team filtration can use that same refresh token to request new access tokens for other Microsoft 365 services (e.g., Outlook, SharePoint) with- out needing the original password again. This maintains access even if the user changes their password. The tool specifically exploits" Family Refresh Tokens" which can bypass certain token binding safeguards, making them even more potent for persistent, flexible access.

3. Evasion Techniques Used by The Attacker

- Distributed Infrastructure (AWS): The tool takes ad- vantage of Amazon Web Services (AWS) the servers are in various geographical regions such as US, Ireland, UK therefor it helps to launch its enumeration and password spraying attempts.Evasion by rotating the source IP addresses of its attack traffic across numerous AWS IPs, Team filtration can evade IP-based blocking mechanisms (which block known malicious IPs) and IP-based rate limiting (which triggers alerts for too many failed logins attempts from a single IP). It also helps to bypass geo-blocking policies by originating traffic from diverse, sometimes less suspicious, regions.

- Low-and-slow and burst Technique: During the password spraying phase, Team filtration often employs config- urable delays between login attempts.
- Abuse of Legitimate APIs and Protocols: Before launching password spraying, attackers need to know which usernames or email addresses are valid within a target organi- zation's Microsoft Entra ID. This is called" user enumeration." The Teams API often has functionalities that allow users to search for or verify the existence of other users within an organization with this the attacker can check if l The Team filtration automates these queries. By sending requests to the Teams API, the tool can analyze the responses. If the API returns a different error message for a non-existent user versus a valid user (even if basic information is withheld), the attacker can deduce which accounts are legitimate.
- Fileless Operations: The core operations of Team Filtration (enumeration, spraying, token acquisition, and API-based exfiltration) do not necessarily involve installing traditional malware files on the target's endpoint. This bypasses tradtional signature-based antivirus and many endpoints detection and response (EDR) solutions that primarily look for malicious files being written to disk or suspicious process executions on the local machine. The attack largely occurs" in the cloud" via API interactions.

Why It Was So Effective

- Team filtration tool uses legitimate APIs, so it looks like normal user behavior.
- No malware was installed-many attack were fileless.
- Attacker targeted cloud-native environment, which traditional antivirus tool cannot monitor.
- Many targets did not have conditional access or auditing enabled.[1][2]

III. RELATED INCIDENTS

Over 80,000 Microsoft Entra ID Accounts Targeted Using Open-Source Team Filtration Tool

Proofpoint threat researchers have recently uncovered an active account takeover (ATO) campaign, tracked as UNK Sneaky Strike, using the Team filtration pentesting framework to target Entra ID user accounts. since December 2024 UNK Sneaky Strike activity has affected over 80,000 targeted user accounts across hundreds of organizations, resulting in several cases of successful account takeover. UNK Sneaky Strike, whose attack campaign peaked in early January with 16,500 accounts targeted in a single day, leveraged AWS servers around the world to deploy the intrusions while using an Office 365 account to facilitate Microsoft Teams API exploitation for account enumeration, an analysis from Proofpoint revealed. Most of the malicious activity arose from IP addresses in the U.S., Ireland, and the UK. Such activity has been associated with Team filtration following the discovery of the tool's rare user agent and OAuth client IDs. Organizations have been urged to defend themselves against potential compromise by blocking erring IP addresses, activating OAuth 2.0 and multi- factor authentication, and implementing Entra ID conditional access policies.[3]

IV. PROPOSED SYSTEM

The Team filtration tool mimic as normal user with valid credential by enumeration and other methods therefore making it difficult to detect by normal methods. Because of that we integrate some tools together to prevent complex and well- planned attack like Team filtration attack and by detecting at- tack we could block the attack. For preventing the multilayered attack by Team filtration, the user integrates Endpoint Detection Response (EDR), security Information and Event Management (SIME), and User Entity Behavior Analytics (UEBA) with this we can create a multilayered defense that is more effective against threat like Team filtration.

EDR (Endpoint Detection and Response): It is a software that is installed on the endpoint such as laptops, desktops, and servers to monitor, detect, and respond to security threats in real time.

Key Features:

- Detects suspicious behavior like unknown programs running.
- Flags fileless attacks, malware, and credential theft.
- Provides forensic data such as logs, timelines, and memory.
- Allows remote isolation of infected machines.

SIEM (Security Information and Event Management): SIEM is software that collects and

analyzes security logs from systems like EDR, firewalls, cloud platforms, user activities, etc.

Key Features:

- Collects and combines logs from many different plat- forms.
- Creates alerts based on rule-based or behavioral detection.
- Enables threat correlation.

UEBA (User and Entity Behavior Analytics): Uses ma- chine learning to establish a baseline of normal behavior for users and systems. If a behavior deviates from the baseline, it flags it as a potential threat.

Key Features:

- Detects anomalous behavior.
- Assigns risk scores to users.
- Often integrated into SIEM.

How Integrating This Will Help? By integrating EDR, SIME, and UEBA it will create a multi layered defense system which will increase the probability of detect, respond, and contain sneaky attack like Team filtration because the Team- Filtration tool attacker uses legitimate tools/Api and fileless technique which could be very hard to find through normal method it will easily get bypass the security system.

How Does It Work Together?

In the above given figure 2 shows how EDR, SIME, UEBA work together. To detect and stop cloud-based identity abuse like Team filtration attacks. What basically happened is EDR detect suspicious process activity like one-drive file triggers power shell or if EDR catches token-stealing tools or unusual script execution it will feed this info to SIME so it can be combined with the other logs. SIME is the central hub where all logs and events are analyzed what SIME dose is it correlates logs from EDR, cloud service (Microsoft 365,

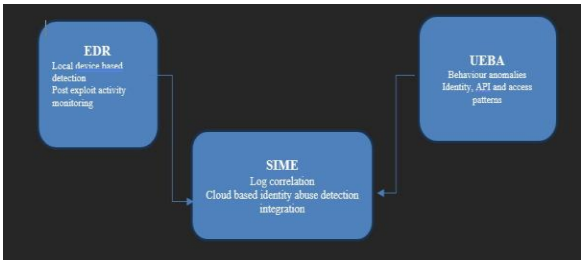

Fig. 2: Integrated Work Flow

Entra Id), UEBA, etc. and after correlating it looks for pattern from all the data that may indicate an attack it also helps us detect identity abuse that crosses from cloud to endpoint and the main purpose of SIME is to organize EDR and SIME and integrate both tools. UEBA understand normal user behavior if anything that does not match the normal behavior it will flag it like odd login time or downloads huge data if something out of behavior happen it sends behavioral alerts to SIME. With this we can prevent attack from Team filtration Tool attack to an extent.

V. CONCLUSION

We investigated how the Team filtration tool and it's been we weaponized and targeted several Microsoft accounts by using, cloud-based strategies take advantage of trustworthy platforms to avoid detection in this‘case study. Integrating SIEM (Security Information and Event Management), UEBA (User and Entity Behavior Analytics), and EDR (Endpoint Detection and Response) offers a multi-layered and intelligent defense, even though traditional security tools frequently fall short. SIEM correlates logs across systems to find hidden threats, UEBA looks for behavioral anomalies that point to identity abuse, and EDR keeps an eye out for post-exploit activity on endpoints. When combined, they provide a proactive method for locating and thwarting advanced threats such as Team filtration.

REFERENCES

[1] M. Langvik," Taking a Dump in the Cloud," Presented at Def Con, Las Vegas, NV, 2021. Available: [Direct URL to the PDF, if known and stable, e.g., https://www.blackhat.com/docs/us-21/arsenal/us-21-Langvik-Taking-A-Dump-In-The-Cloud.pdf

[2] Proofpoint Threat Research Team, " Attackers Unleash Team filtration: Account Takeover Campaign (UNK Sneaky Strike) Leverages Popular Pentesting Tool," Proofpoint, May 2024. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/attackers- unleash-Team filtration-account-takeover-campaign

[3] R. Lakshmanan," Over 80,000 Microsoft Entra ID Accounts Targeted Using Open-Source Team filtration Tool," The Hacker News, Jun. 2025. [Online]. Available:

https://thehackernews.com/2025/06/over-80000-microsoft- entra-id-accounts.html

[4] M. Langvik. (2023, Nov. 7). Team- Filtration (v3.5.0) [Computer soft-ware].Available:https://github.com/Flangvik/Team filtration/ releases/tag/v3.5.0

[5] Microsoft," Azure Identity Management and access control security best practices," Microsoft Learn, May 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best- practices