baseVISION TI Report

Hijacking Microsoft Company Accounts via TikTok Open Redirection Abuse Is Still a Thing

baseVISION

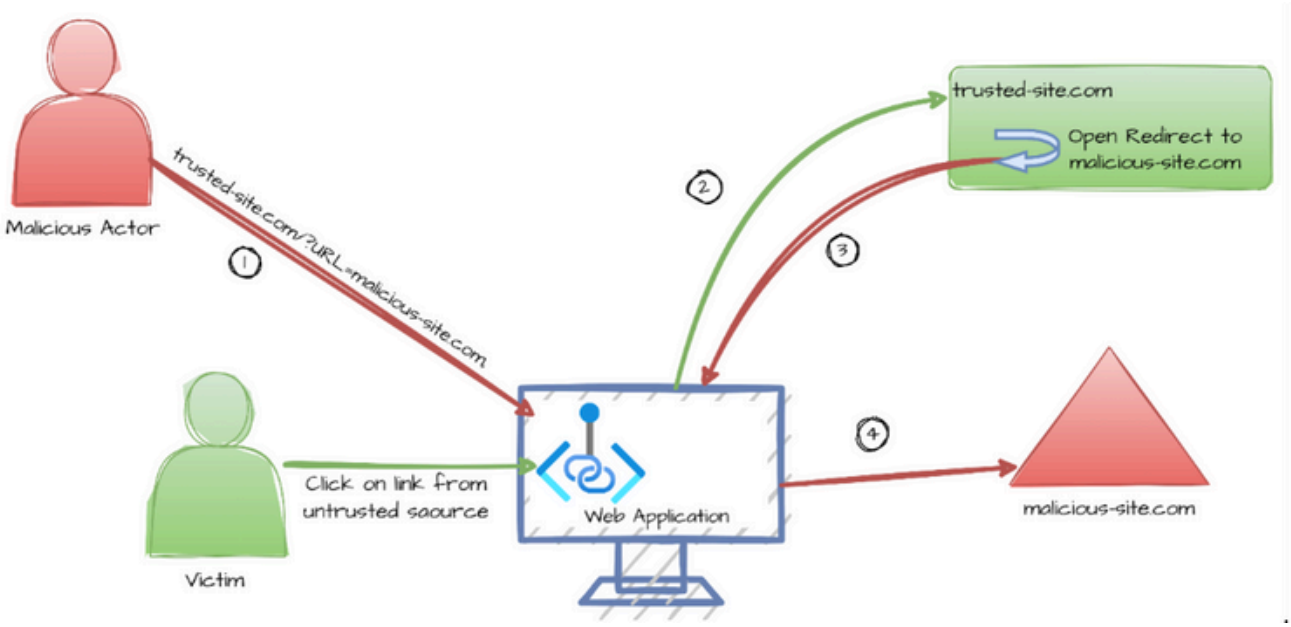
Cybercriminals are continuously trying to exploit legitimate platforms in deceptive ways to hijack Microsoft credentials. In July 2025, our team at baseVISION uncovered a stealthy phishing campaign that leverages TikTok open redirect vulnerabilities to compromise Microsoft accounts, using seemingly legitimate URLs to deceive users and lead them to untrusted webpages to harvest credentials. Nothing new under the sun: similar campaigns were noted by other researchers in 2024.

Campaign Overview: from Suspicious Sign-In Alerts to Malicious Email Lures

We have observed a consistent pattern across multiple customer environments, with alerts triggered by failed login attempts from an unusual geographic locations. These login attempts specifically targeted Microsoft OfficeHome application, and shared axios/1.10.0 as the common user agent string, which is frequently associated with automated tools in credential harvesting attacks.

Further investigation revealed that targeted users had received emails from the same sender, with similar business-related subject line regarding a "Completed Sales Contract". These emails also contained a PDF attachment and a disguised URL embedded in the email body.

How Does The Redirect Work?



Example of diagram: CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

The embedded URL looked roughly like this:
hxxps://www.tiktok[.]com/%2F%2Flink/v2?aid=1988&lzdlang=enFSmPWg&scene=bio_url&target=[LINK]

The above URL is TikTok's official redirect service for external links normally placed in user bios. Even though it is normally used for legitimate purposes, it can be abused in the target= parameter due to lack of input validation. As a matter of fact, the final URL destination does not get validated and restricted to whitelisted domains, exposing a classic open redirect vulnerability. This issue was already disclosed by security researchers in the past, and in our observed cases, the redirect functionality was further chained with a Google redirector to obfuscate the final malicious domain. As an example of this multi-stage redirect chain:

hxxps://www.tiktok[.]com/%2F%2Flink/v2?aid=1988&lzdlang=enFSmPWg&scene=bio_url&target=google[.]com[.]gt/travel/clk?...&pcurl=...

- **target=google.com.gt/travel/clk?**: is a known Google redirect layer, which in our incident also contained "%5C", the URL-encoded backslash character \, commonly used for obfuscation purposes in redirect chains; Here, it points to a Google domain for Guatemala (google.com.gt) with a path (/travel/clk?...) that suggests a click-tracking, often used in advertising, but could be repurposed for IP-based cloaking and IP-based filtering to evade detections.
- **pcurl**=...: Parameter for the phishing campaign pointing to the malicious domain. This redirects to the payload domain "ligerteknoloji[.]com[.]tr" (with a VirusTotal score of 6/94), and both a folder path and a Base64-encoded string that decodes to the targeted user's email address.
- **aid=1988**: Likely a tracking ID used by TikTok to identify the source of the link such as a specific user or campaign. However, even though multitude of users are seen with similar usernames, no user could be found with this exact tracking ID.

- **lzdlang=enFSmPWg:** In legitimate systems, parameters like lang or similar are used to specify language or localization settings (lang=en for English). However, **lzdlang=enFSmPWg** is non-standard and includes a random string (enFSmPWg). This could serve as a unique identifier for a specific phishing campaign allowing attackers to track clicks or tailor the attack. Furtermore, this could also be used as obfuscation technique to evade pattern-based detection, the random string makes the URL unique, reducing the likelihood of it matching known malicious patterns in security databases.
- **scene=bio_url**: Indicates the link is intended to appear as if it originates from a TikTok user's bio.

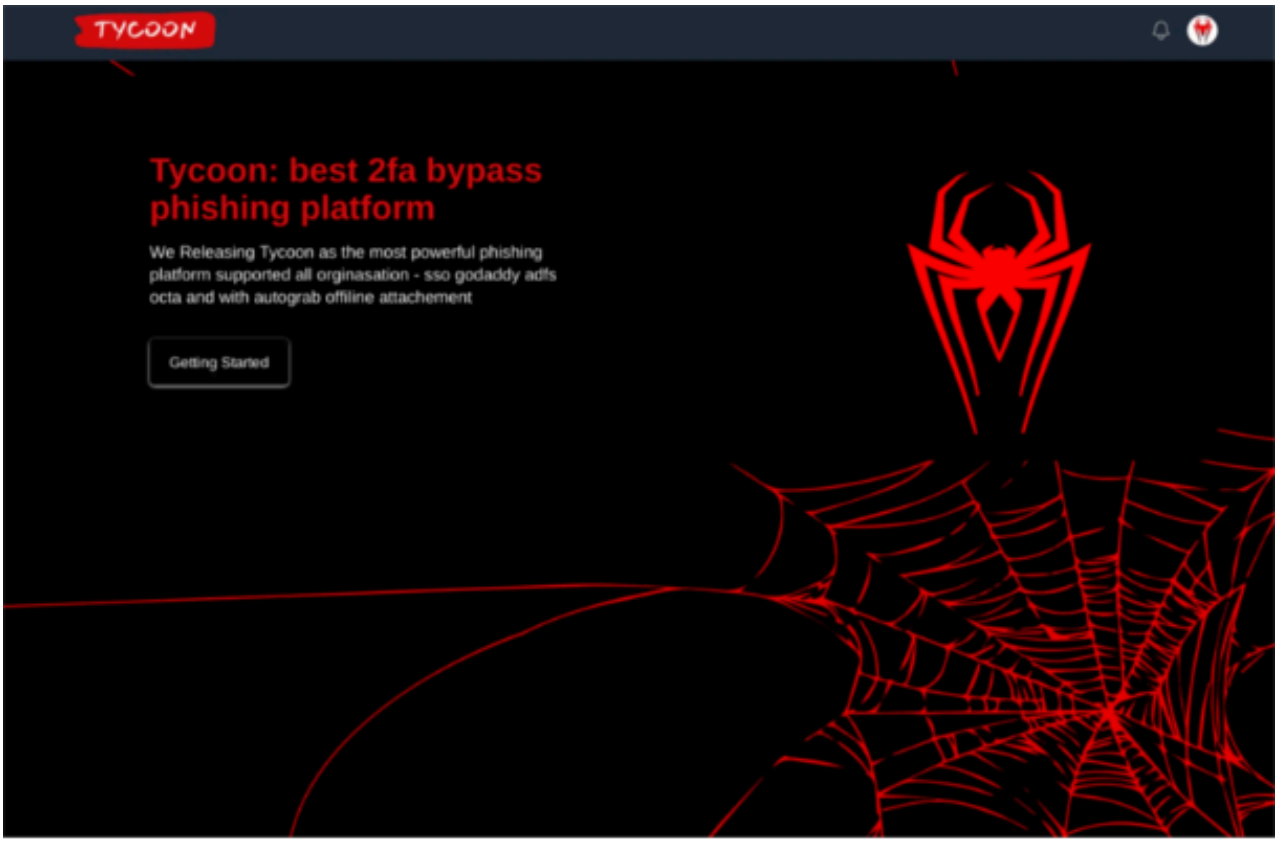
Once the user clicks the link and connects to the phishing domain, they're taken through a Cloudflare CAPTCHA verification step.

- When solving the CAPTCHA from an Azure IP address, the website redirects the user to a non-suspicious destination, effectively serving benign content;
- When performing the CAPTCHA from a residential IP address, the user gets routed to a malicious landing page that serves the actual malicious payload.

This tactic, known as IP-based filtering or IP-based cloaking, is a common evasion technique used by attackers. Requests from cloud infrastructure IPs, such as those from Azure, are served benign content, as these IPs are often linked to security tools and monitoring systems. By doing so, attackers aim to preserve the reputation of their infrastructure and avoid detection. In contrast, requests from residential IPs, which are typically associated with real users, are deemed safe targets and are redirected to the actual malicious payload.

Once the phishing domain has been reached, users are presented with an Adversary-in-the-Middle (AiTM) phishing page, a convincing replica of a corporate-branded Microsoft 365 login, aimed at stealing corporate credentials (and possibly session cookies).

Possible Attribution



The 2023 Tycoon PhaaS platform website at tycoongroup[.]ws

One possible attribution for this campaign points to the Tycoon 2FA phishing-as-a-service (PhaaS) platform, which has been actively used by the financially motivated threat group Storm-1747. The structure of the TikTok redirect URL observed in this case matches URLs previously documented in sandbox analyses by ANY.RUN.

Recent samples from July 2025 (i.e., example 1 and example 2) shows an identical redirect chain beginning with "hxxps://www[.]tiktok[.]com/link/v2?aid=1988&lzdlang=enFSmPWg&scene=bio_url&target=", and leading to the same phishing URL, confirming its use within a Tycoon 2FA phishing campaign.

Tycoon is known for leveraging advanced Adversary-in-the-Middle (AiTM) techniques to intercept both credentials and session tokens, effectively bypassing multi-factor authentication. The use of open redirects, CAPTCHA challenges via Cloudflare and Microsoft 365-themed lures are all related to this threat actor, reinforcing the likelihood of its involvement in this operation.

Storm-1747:
This threat actor is involved in phishing operations for financial gain. They utilize the Tycoon 2FA PhaaS (Phishing-as-a-Service) designed to bypass multi-factor authentication (MFA) protections, particularly targeting Microsoft 365 and Gmail accounts.

Aliases: Saad Tycoon Group, Tycoon Group, SaaadFridi, Mr_XaaD, Dadsec OTT

Country: Worldwide

IOCs

- hxxps://www.tiktok[.]com/%2F%2Flink/v2?aid=1988&lzdlang=enFSmPWg&scene=bio_url&target=google[.]com[.]gt/travel/clk?...&pcurl=...
- ligerteknoloji[.]com[.]tr
- xjrsel[.]ywnhwmard[.]es
- Teksystem[.]com[.]tr

baseVISION

Conclusion

TThis campaign highlights how threat actors can cleverly chain multiple legitimate services to disguise their credential-harvesting operations. By abusing trusted platforms, particularly those with open redirect vulnerabilities, attackers increase their chances of bypassing security controls and deceiving end users. TikTok's redirect functionality continues to be a favored tool in these campaigns due to its widespread trust and flexible redirection logic. To defend against these threats, security teams must remain vigilant and adapt their detection strategies to account for multi-stage phishing techniques that rely on evasion and redirection. At the same time, end users should be regularly educated on the risks of blindly trusting even well-known domains, since threat actors increasingly weaponize familiar infrastructure to gain initial access.

What you can do next

Cybercriminals continue to exploit open redirect vulnerabilities and sophisticated cloaking techniques to bypass security controls. To protect your organization and users:

1. Review Your Redirect Policies: Audit your own web applications for open redirect vulnerabilities (e.g., CWE-601) and ensure proper input validation and domain whitelisting.
2. Educate Your Users: Share this blog post with your colleagues and raise awareness about deceptive redirect chains and AiTM phishing tactics.
3. Enable Advanced Threat Protection: Use Microsoft Defender for Office 365 or similar tools to detect and block malicious links and credential phishing attempts.
4. Monitor for Suspicious Sign-Ins: Set up alerts for unusual login patterns, especially from unexpected geographies or using known malicious user agents like axios/1.10.0.