# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | LogoKit leverages open-redirection bug for phishing

**Tracker ID:** TN0815 **Date:** 12/August/2022 **Category:** Cyber Attack - Phishing **Industry:** All **Region**: All

### Background

Threat actors have been found leveraging Open Redirect Vulnerabilities in online services and applications to evade spam filters and send phishing content in a new way. Using highly trusted service names such as Snapchat and other internet services, they constructed customized URLs that connect to malicious pages containing phishing kits. The discovered kit is known as LogoKit, and it has previously been used in attacks against Office 365, Bank of America, GoDaddy, Virgin Fly, and a variety of other significant financial institutions and internet services throughout the world.

LogoKit is well-known for its use of JavaScript to create dynamic content. It can change the logos (of the impersonated service) and text on landing pages in real-time to adjust on the fly, boosting the user's likelihood of engaging with the malicious resource. Attackers frequently exploit domain names in exotic jurisdictions or zones with inadequate abuse control mechanisms (.gq,.ml,.tk, ga,.cf) to get unauthorized access to legitimate web pages and then use them as hosts for further phishing dissemination.

LogoKit delivers phishing URLs to users, including their email information. When a victim hits the URL, LogoKit pulls the company's logo from a third-party service, such as Clearbit or Google's favicon database. The victim's email address is then auto-filled in the email or username box, making them believe they have already signed in. If the victim enters their password, LogoKit initiates an AJAX call, sending the victim's email address and password to an external source before redirecting them to their "legitimate" company website.

To prevent detection, it disguises malicious activity as legitimate service notifications, tricking the victim into visiting the malicious resource. The actors are utilizing their access to hacked web resources to place phishing without the owners' knowledge. Unfortunately, exploiting Open Redirect vulnerabilities aids LogoKit dissemination because many (even popular) web services do not consider such vulnerabilities significant, and in some cases, do not even patch them, leaving the door open for such exploitation.

### MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, and Exfiltration.

### Indicators of Compromise *

Please refer to the attached sheet for IOCs.

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | LogoKit leverages open-redirection bug for phishing

**Tracker ID:** TN0815 **Date:** 12/August/2022 **Category:** Cyber Attack - Phishing **Industry:** All **Region**: All

### Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Validate the IOCs attached and implement the detection & prevention accordingly.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Educate employees on how to protect themselves from the ongoing phishing threats.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Perform a thorough vulnerability assessment to identify such weaknesses beforehand.

### References


- CYBERCRIME INTELLIGENCE, LogoKit Update – The Phishing Kit Leveraging Open Redirect Vulnerabilities, Resecurity, 07th August 2022, External Link (resecurity.com).
- Alessandro Mascellino, Hackers Exploit Open Redirect Vulnerabilities to Conduct LogoKit Phishing Campaigns, Infosecurity, 08th August 2022, External Link (www.infosecurity-magazine.com).


In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

*

| Domain | URL |
|---|---|
| fleek[.]co | http[:]//email25.godaddy[.]com-sign-realm.getforge[.]io/ |
| storageapi.fleek[.]co | |
| institutoaxioma.com[.]ar | |
| csb[.]app | |
| web[.]app | |
| us[.]archive[.]org | |
| gl1hz[.]csb[.]app | |
| ia801507[.]us[.]archive[.]org | |
| cerstts[.]ga/100/wgbground | |



#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia