ORACLE

Technical insights into the KissFraud scheme

With the help of the Parallel Graph AnalytiX (PGX) team and Oracle Labs researchers, Oracle Moat IVT has identified a context spoofing fraud that redirects traffic to counterfeit news sites.

Authors:
Rhicheek Patra, Senior Research Manager, Oracle Labs
Iman Ait Chikh, Technical Staff, Oracle Labs

April 2022

The recent KissFraud scheme discovered by Oracle Moat IVT is a context spoofing ad fraud scheme that leads advertisers to believe ad impressions have occurred on a safe, reputable news site. In reality, the ad impressions are happening on multiple malicious websites that host pirated video content.

The Oracle Moat IVT team uncovered this scheme using our patented Graph Machine Learning techniques with a focus on Explainable Representation Learning. (The Explainable Representation Learning model was developed jointly with the Parallel Graph AnalytiX (PGX) team and researchers at Oracle Labs.

KissFraud **r**edirection **s**trategy: Divert **r**eal **u**sers to **c**ounterfeit **s**ites

The core mechanics of the KissFraud scheme redirects human viewers of pirated video content to counterfeit "news" sites. The fraud scheme is comprised of the following two categories of websites: Video sites for pirated TV shows and counterfeit news sites. Styles incorporate information about spacing, tabs, and fonts and are critical to preserving the template's design. Place cursor to see name of style applied.

Two categories of websites

VIDEO SITES FOR PIRATED TV SHOWS	COUNTERFEIT NEWS SITES
kimcartoon[.]li	kisscenter[.]net
kissasian[.]li, kissasian[.]mx	kissorg[.]net
kisstvshow[.]to	ksnews[.]me

Table 1. The two categories comprising the KissFraud scheme.

If accessed directly, the counterfeit news sites display copied content from legitimate news sites. Because the content has been copied from a legitimate site, the counterfeit news sites display what appears to be brand-safe content along with a URL that resembles the title of the copied news article. At first glance, the counterfeit news sites suggest a relevant and safe ad environment.

However, when a user navigates to the streaming sites in search of pirated TV shows and clicks on an episode or movie link, they will be redirected to one of the counterfeit news sites. To the user, the webpage still looks like the streaming site they previously visited, but the page URL has changed to one of the counterfeit news site domains.

Advertisers relying on URLs and page content analysis for ad tracking might be misled by this context spoofing scheme and tricked into believing that their ads are displayed next to legitimate news articles, with impressions generated by users interested in those news articles. Instead, ads are actually viewed next to pirated video content. In short, the ad impressions are not coming from users interested in news articles but rather users watching pirated video content.

These redirections to counterfeit news sites create millions of weekly ad impressions in our footprint. It's reasonable to assume the impact is much greater since we do not measure every ad appearing on these counterfeit sites.

KissFraud scheme: Step by step

As shown in the diagram below, when a user who wants to view pirated TV shows clicks on an episode or movie link, they are redirected to the counterfeit news website. Relative links such as the following are used:

```
<a rel="noreferrer no opener" href="/Cartoon/Crossng-Swords-Season-2/Episode-10-Hard_Days-Knight?id=103811" title=Watch Crossing Swords Season 2 Episode 10 — Hard Days Knight online">Episode 10 — Hard Days Knight</a>
```

The following flow diagram shows how the KissFraud scheme works using an example from kimcartoon[.]li, one of the malicious websites identified by the Oracle Moat IVT team.

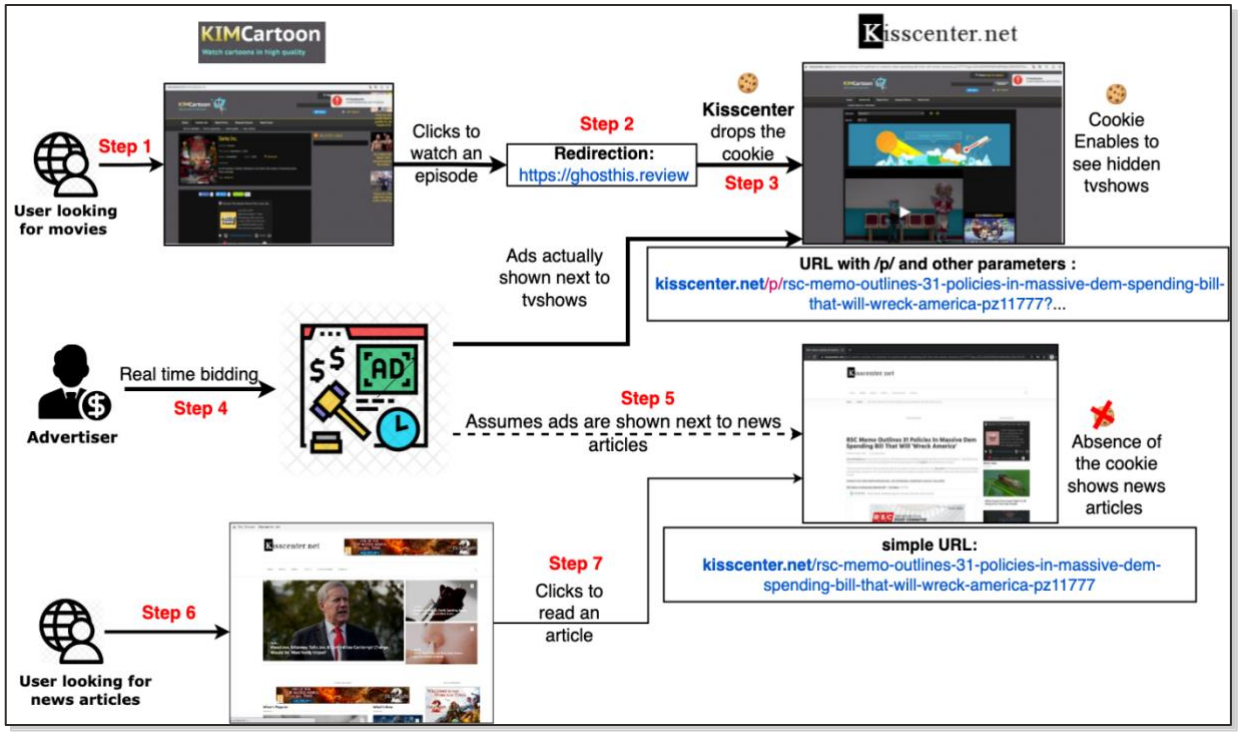

Figure 1. KissFraud flow diagram.

The flow diagram in Figure 1 shows the kisscenter fraud scheme from three perspectives (the steps are highlighted in red in Figure 1.).

A breakdown of each step within the KissFraud scheme

User searches for pirated TV show content

Step 1: A user, looking for pirated TV show content using a search engine, arrives at the fraudulent streaming site kimcartoon[.]li and clicks on the video they want to watch.

Step 2: The user is automatically redirected via ghosthis[.]review to a URL indicating a news article on the counterfeit news site kisscenter[.]net. To the user, the page content still looks like kimcartoon[.]li.

Step 3: The page kisscenter[.]net drops a cookie in the user's browser which prevents the counterfeit news content on kisscenter[.]net from loading, displaying only the pirated TV content.

Advertiser impact

Step 4: The advertiser bids on and buys ad space on kisscenter[.]net relying on page content, user traffic and URL to determine the value of the ad inventory.

Step 5: The content on kisscenter[.]net looks safe from any context analysis or investigation tools due to the absence of cookie that *only* gets dropped on redirection from kimcartoon[.]li.

User looking for news articles

Step 6: Some users arrive at kisscenter[.]net by browsing the web, although statistics indicate a smaller than usual percentage of users coming from searches for a legitimate news site.

Step 7: These users only see the news content and do not see any pirated TV content from kimcartoon[.]li because of the absence of the cookie that gets dropped only during the redirection.

Obfuscating the referring domain

The fraudsters use an intermediate lookup service hosted at ghosthis[.]review. This is done to obfuscate the referring domain (i.e., we would not observe kissasian[.]li as the referring domain on the counterfeit news sites). However, knowing how redirections are done, the KissFraud scheme can be verified by checking if a large percentage of a suspected counterfeit news website has referrals from ghosthis[.]review.

The URL after the redirection (where the pirated video content is displayed) might look as follows:

https://kisscenter[.]net/p/rsc-memo-outlines-31-policies-in-massive-dem-spending-bill-that-will-wreck-america-pz11777?sig=U2FudGEtSW5jfHx8RXBpc29kZS01fHx8MTYzODc4MzQ3NA==&id=103712&op=cnc

Some notable insights from the URL

- **kisscenter[.]net** is the counterfeit news site, redirected from kimcartoon[.]li
- **/p/** path element only appears after redirection, i.e., when accessing the counterfeit news site directly, URLs typically do not have a '/p/'.
- **rsc-memo-outlines-31-policies-in-massive-dem-spending-bill-that-will-wreck-america-pz11777** → URL suggests an article on some policies regarding spending bill. On further investigation, we found that only the -pzXXXXX part determines which article is shown on the counterfeit news site and ghosthis[.]review seems to randomly pick an "article" for the selected episode.
- The **sig** parameter seems to be leveraged in combination with the cookie.
- The **id** parameter seems to identify the video

Cookie mechanism used to hide pirated video content

If referred to by ghosthis[.]review, the counterfeit news site will drop a specific cookie on the user's browser. The cookie ensures that it is not possible for the user to view the original counterfeit news articles pointed to by the URL.

How Graph Machine Learning discovers and detects ad fraud

Because detecting context spoofing ad fraud is a challenging endeavor, simple rule-based approaches do not suffice. Elaborate fraud schemes, such as this one, can easily mask their context and traffic sources, allowing fraudsters to dupe advertisers into buying their falsified ad inventory. In collaboration with Oracle Moat IVT, the Parallel Graph AnalytiX (PGX) team at Oracle Labs developed advanced machine learning techniques for ad fraud detection.

PGX is a toolkit for graph analysis, supporting supervised and unsupervised explainable graph machine learning (ML) algorithms such as GraphSage, DeepWalk and patented (unsupervised) explainability techniques. Furthermore, PGX supports built-in algorithms such as pagerank or community detection algorithms and fast SQL-like graph pattern matching queries. The Graph ML techniques are available in Oracle Property Graph or OCI Data Science environment.

The advantage of Graph ML over traditional machine learning approaches lies in the possibility to leverage complex relations between data points. Graph ML is applicable in a wide range of use cases, including recommender systems for social networks or shopping, anomaly detection for bank fraud and malware detection, or named entity disambiguation using graph embeddings.

This blog post from the Oracle AI and Data Science blog illustrates a Graph ML pipeline for intrusion detection (detecting malicious activity in network traffic). The pipeline steps include building graph files from raw data, using graph algorithms to extract rich features from graph data and applying OML's Auto ML capabilities for the classification task. In a related security analytics use case with Oracle SaaS Cloud Security (SCS), PGX is used to detect malicious processes in event logs of server instances.

More details on Oracle SaaS Cloud Security capabilities can be found here: "Using graph powered security analytics to find attackers quickly." Graph ML is also applicable in the health care domain. This blog post on Graph Machine Learning for enhanced healthcare services gives an overview from knowledge graph construction to graph-powered diagnosis prediction.

Explainable Graph ML is especially relevant in non-academic settings where actions are taken based on predictions of ML pipelines. For a malware detection use case, it is important to understand why the model flagged a certain data point as an anomaly to avoid acting on false positives.

Ultimately, the Oracle Moat IVT team's domain expertise, in combination with the Oracle Labs technology capabilities, made it possible to identify the KissFraud context spoofing scheme. Working in tandem with the Parallel Graph Analytix team and Oracle Labs researchers enables Oracle Moat IVT to be on the cutting edge of innovation—leading the fight against ad fraud.

To learn more about how Oracle Moat can help protect the quality of your inventory, reputation, and revenue potential, visit our website and contact us today.