Success story

Protection against online fraud on all key web resources: Collaboration with Tutu.ru

Tutu.ru is an online travel service where you can buy train, plane, and bus tickets, book hotels, and purchase holiday packages. The site has been operating since 2003 and has one million visitors per day.

The problem

Tutu.ru employees started receiving complaints from customers who had come across phishing websites that fed off Tutu.ru's brand. Specifically, the websites imitated either Tutu.ru's products or name, offering tickets at a 70% discount. The fake websites did not have or sell any real tickets, of course — it was merely a way to steal customer data.

Fighting alone

The situation was made more complicated by the fact that Tutu.ru has one million visitors per day and each of them could potentially fall victim to the scam.

Tutu.ru tried to protect their brand on their own: they detected where the data was parsed from (the threat actors had to show something to the customers) and blocked these addresses. The measures had only a temporary effect, however. The fake websites were quick to revive. The company's specialists worked with registrars, hosting service providers, and advertising networks, but in the words of Vadim Melnikov, Technical Director at Tutu.ru, it was 'time-consuming, painful, and ineffective'.

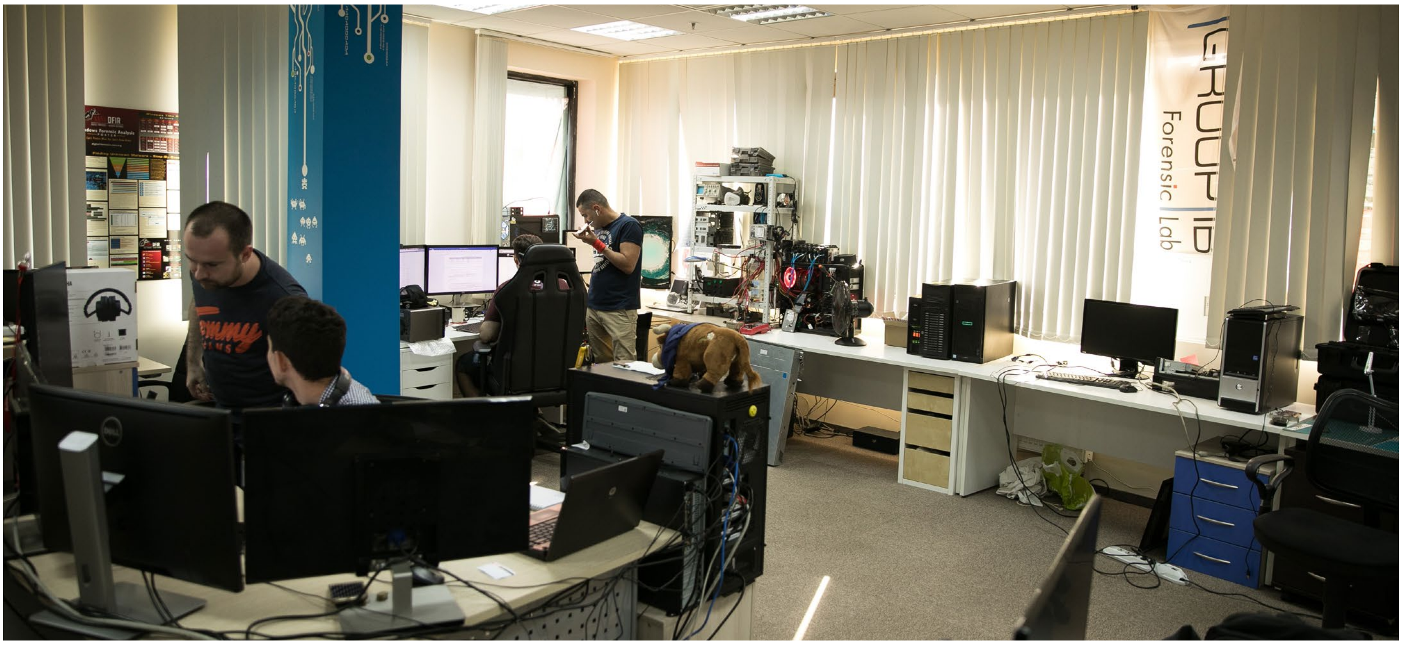
It became clear that solving the problem by engaging the employees was impractical. The company did not have a separate department to deal with such issues and the time the employees spent on dealing with the situation could be devoted to more important business tasks.

Description of the fraud:

The threat actors copied the original website's design (or deployed it within an iframe) and hosted the copy at a similar-looking URL. They then created ads on Google and Yandex that featured the genuine domain. Once an ad was approved, they substituted the real domain with a phishing one.

The hackers took a similar approach to mobile apps, copying their design and placing links for downloading cloned apps on official and unofficial platforms, in social media groups, and in contextual ads. Once users installed the app, they had their personal data stolen, in some cases even their money.

> **We first experienced this problem as early as 2015. After receiving recommendations from our colleagues in the industry, we decided to reach out to Group-IB's Brand Protection team. We liked the pilot project and have been working together ever since.**
>
> **Vadim Melnikov,**
> Technical Director, Tutu.ru



What Group-IB did

We offered Tutu.ru our Brand Protection solution to protect their brand against fraud.

- **We detected more than 12,000 domain names that looked similar to Tutu.ru.**

  We work with major domain name registrars that provide regular updates about new websites in the .ru segments of the Internet. As a result, our database of functioning domains is always up to date. To discover third-level domains or domains in a certain geographical area, we use passive DNS technology, which collects data about DNS queries.

- **We analysed linked websites in terms of their risk level and listed them by order of response priority.**

  When a web resource posed a real threat, we took the required steps to block it. Even if linked resources did not show any signs of fraud at the time of detection, we monitored them using automated tools. As such, the moment that a threat actor decided to use a domain exploiting Tutu.ru's name, we detected it and took the necessary measures.

- **We detected more than 2,000 ads and mobile apps targeting Tutu.ru.**

  Although not every single one was initially fraudulent, each resource was automatically and regularly monitored since any such offers pose a potential threat to the brand.

Group-IB's Brand Protection results

- **We blocked 100% of resources, that could potentially cause or did indeed cause damage to the brand and its customers:**
  - 150 websites and malicious mobile apps
  - Infringing content on web resources that breached Tutu.ru's copyright.

- **150 websites blocked**
- **12,000 similar-sounding domain names detected**
- **2,000 ads and mobile apps detected and monitored**

- **We recovered traffic to the official Tutu.ru website**

> **At Tutu.ru, we care about our customers and strive to protect them from financial losses. Loyal customers of our online travel service will not be misled by fraudsters that exploit Tutu.ru's name.**

Vadim Melnikov,

Technical Director, Tutu.ru

Group-IB is one of the leaders in detecting and preventing cyberattacks, exposing fraud, and protecting intellectual property online.

Unique threat intelligence data and proprietary solutions for tackling cybercrime are at the core of Group-IB's products and services. The continuous development of online threat detection mechanisms has helped protect more than 200 Russian and international brands.

According to Gartner, IDC and Forrester, Group-IB is one of the key threat intelligence providers in the world, with a database of more than 100,000 threat actor profiles.

55 000+
Hours of Incident Response

1000+
Investigations woldwide

EUROPOL INTERPOL Official partner

OSCE Recommended by the Organization for Security and Co-operation in Europe (OSCE)

Learn more about our Brand Protection:

group-ib.ru/brandprotection

info@group-ib.com