Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

Company

Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

EUROPOL INTERPOL

Official EUROPOL and INTERPOL partner

OSCE

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

WORLD ECONOMIC FORUM

Member of the World Economic Forum

1000+

successful investigations worldwide, 150 of which were of special complexity

$300 million

was returned to our clients due to Group-IB's efforts

Forrester Gartner

According to Forrester and Gartner, Group-IB Threat Intelligence is among the best services in the world

BUSINESS INSIDER

One of the top 7 most influential cyber security companies according to Business Insider UK

IDC

Leader of the Russian Threat Intelligence Market

Media coverage:

theguardian Bloomberg Forbes REUTERS

Esquire CNN The Register Biting the hand that feeds IT InformationWeek DARKReading SC MAGAZINE

Products & Services

EARLY WARNING SYSTEM

- Threat Intelligence
- TDS
- Secure Bank
- Secure Portal

PREVENTION

- Security audit
- Compromise Assessment
- Red Teaming
- Brand Protection
- Antipiracy

RESPONSE 24/7/365

- Computer Emergency Response Team CERT-GIB

INVESTIGATION

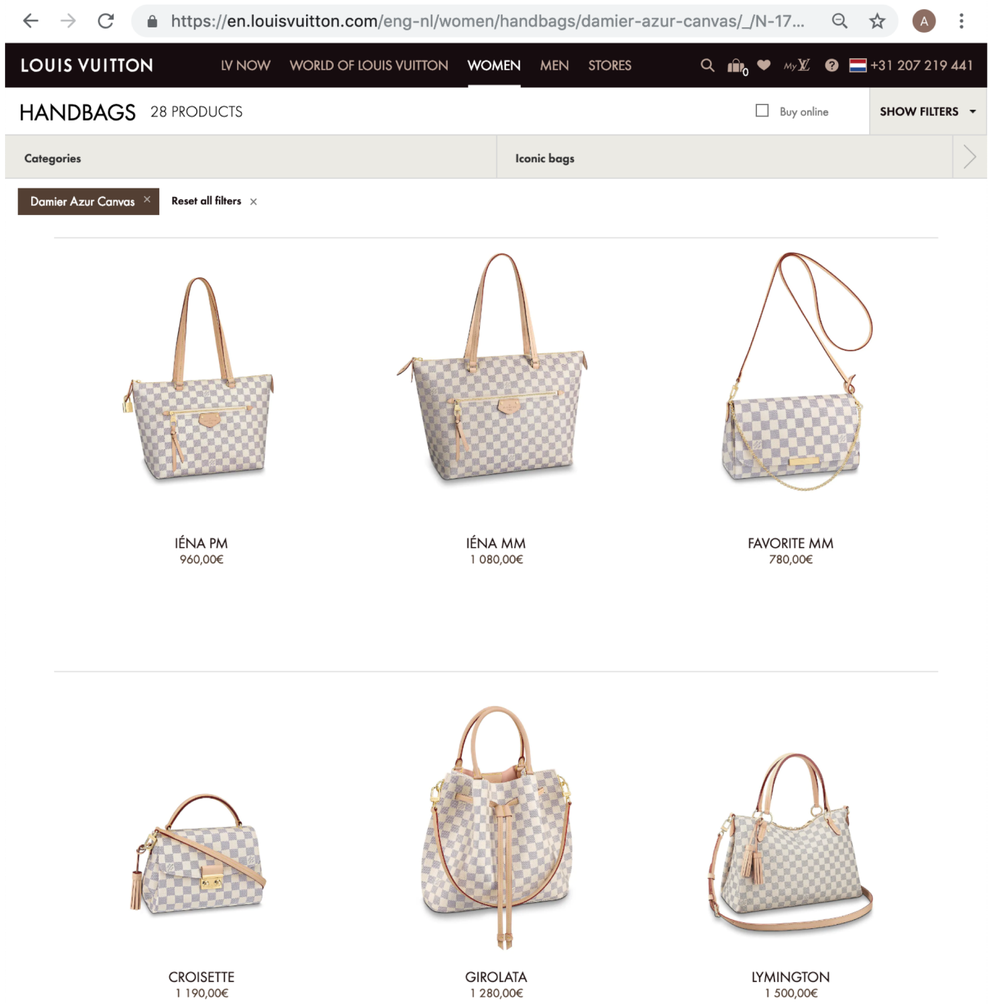
- Digital forensics and malware analysis
- Incident investigation
- Financial and corporate Investigation

Powered by threat intelligence data, Group-IB products and services complement each other resulting in a synergetic outcome and high efficiency of combating cybercrime.

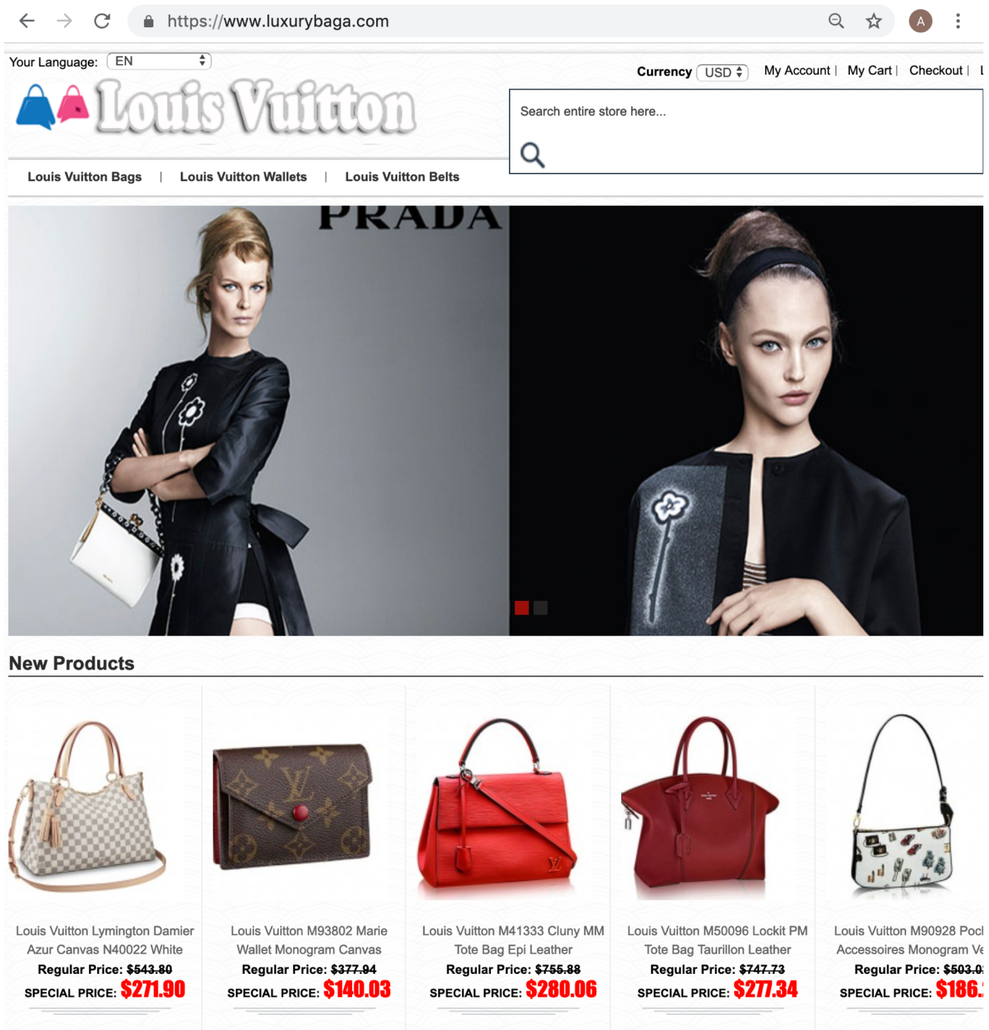
IPLegist

Intellectual Property Protection Platform

PROBLEM



VS

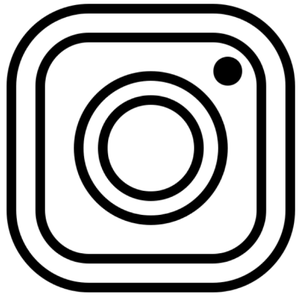


Authentic

Counterfeit

IPLegist
Intellectual Property Protection Platform

PROBLEM



Brand Abuse

The problem which we are trying to solve is the problem of Intellectual Properties misuse. A lot of companies are suffering from intruders which are using their brand illegally, earning money and corrupting companies reputation.

Piracy

Another case is when pirates are uploading digital content like music or brand-new movie to the torrent tracker or a pirate website. Content creators are losing money, while pirates are earning them using cam-rips.

Counterfeit

A huge number of non-original products of famous brands are sold on dubious resources on a daily basis, damaging the reputation and the name of the companies-owners.

IPLegist
Intellectual Property Protection Platform

ONLINE THREATS TO BRANDS

Internet fraud, illegal use of brands

Fraudulent websites, cloned websites, phishing

Fake accounts and groups on social media

Fake mobile apps

Fake partnerships

Illegal advertising


БИЗНЕС / КИБЕРБЕЗОПАСНОСТЬ 14.04.2017 12:43

Атака клонов: как работают схемы с фейковыми сайтами «Роснефти» и других крупных компаний

155 SHARES ОБСУДИТЬ

Илья Сачков Forbes Contributor

Фото: REUTERS / Jason Lee

Злоумышленники создают копии сайтов российских корпораций, чтобы заключать контракты от их имени. Средний ущерб от такой атаки – от 1,5 млн рублей

$7,500,000,000+

Annual loss suffered by companies due to brand abuse in Russia

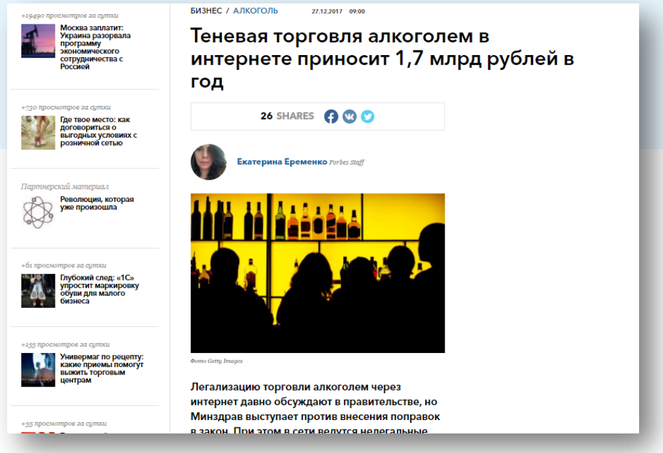
Forbes

Illegal online sales

Offers of counterfeit sales

Grey import

Breaches of partnership agreements


БИЗНЕС / АЛКОГОЛЬ 27.12.2017 09:00

Теневая торговля алкоголем в интернете приносит 1,7 млрд рублей в год

26 SHARES

Екатерина Еременко Forbes Staff

Фото: Getty Images

Легализацию торговли алкоголем через интернет давно обсуждают в правительстве, но Минздрав выступает против внесения поправок в закон. При этом в сети ведутся нелегальные

$1,500,000,000+

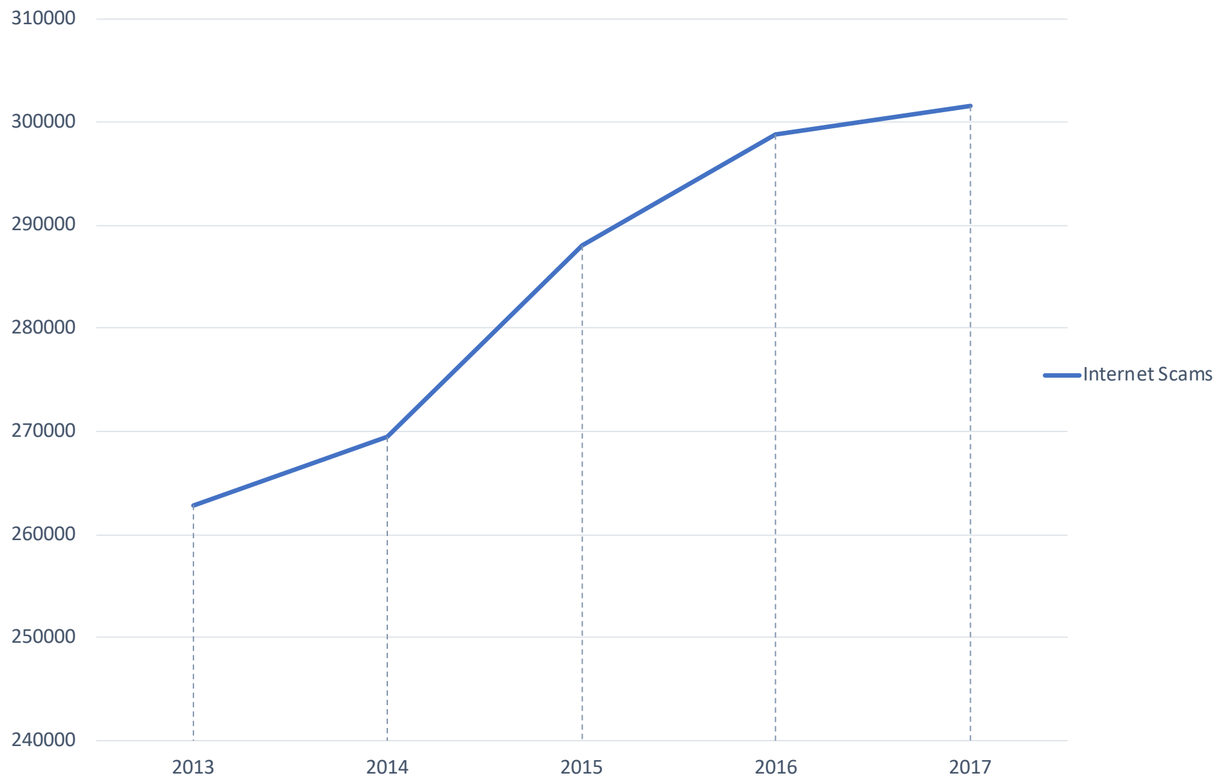
Market value of online sales of counterfeit goods in Russia in 2017

Forbes

IPLegist
Intellectual Property Protection Platform

PROBLEM

The Complaints on Internet Scams



According to Internet Crime Complaint Center

Retail

PROMOTION METHOD
Contextual advertising

NUMBER OF SEARCHES
(per week)
10,000

ADVERTISING EFFECTIVENESS
(views compared to clicks)
14%

CONVERSION RATE
(purchases compared to visitors)
9%

AVERAGE PURCHASE PRICE
$30

$4,000

Losses Caused by Scammers in One Week

Financial Sector

PROMOTION METHOD
Phishing targeted at subscribers of the bank in social media

NUMBER OF POTENTIAL VICTIMS
50,000

RATE OF COMMUNICATING WITH VICTIMS
150 people per day

PERCENTAGE OF TRUSTING CLIENTS
1%

AVERAGE AMOUNT STOLEN FROM A BANK CARD
$1,000

$11,000

Manufacturing

PROMOTION METHOD
Targeted email newsletter

NUMBER OF RECIPIENTS
1,000

EFFECTIVENESS OF EMAIL BLASTS
20%

CONVERSION RATE
(purchases compared to visitors)
9%

AVERAGE ORDER PRICE
$760

$13,000

IPLegist
Intellectual Property Protection Platform

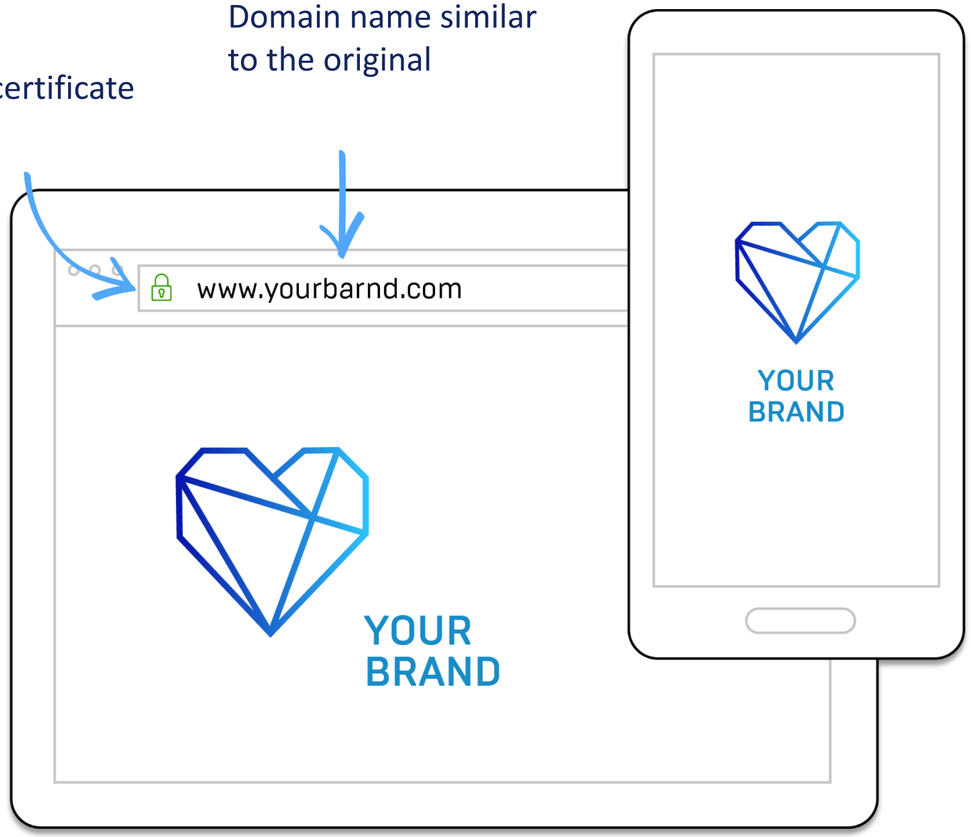
HOW CRIMINALS PROFIT FROM YOUR BRAND

1 THEY CREATE A PLATFORM

- Logo, trademarks
- Name
- Brand colours

Domain name similar to the original

SSL certificate



2 THEY ATTRACT TRAFFIC

Search Engine Optimisation (SEO)

Advertising
- Contextual
- Banner
- On social media
- Through Adware

Spam
- By email
- In messengers

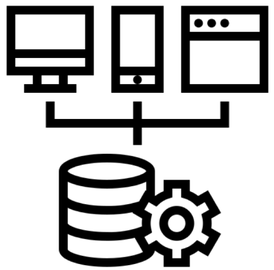
Promotion on social media
- Using fake brand accounts
- Using bots
- Through opinion leaders

IPLegist
Intellectual Property Protection Platform

SOLUTION

IPLegist was born in February 2018 as a spin-off project inside Group-IB, an intelligence-driven cyber security company with 15 years' experience in high-tech crime investigation.

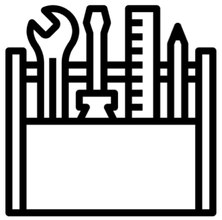
In summer 2017 the Group's Threat Intelligence (recognized by Gartner, Forrester, IDC and Research&Markets) detected a dramatic rise in the number of illegal brand usage targeting large banks and major corporations. That's when things got serious.



Our solution is the Intellectual Property protection platform which combines advanced monitoring system and prevention toolkit. Customers will be able to find IP misuse and shut down illegal activities by themselves within the law.

With our toolbox clients will save money, reputation and trust of their customers, because the number of such fraudulent cases will significantly decrease after implementation of our toolbox in the companies' business processes.

Advanced monitoring system is specifically tailored for automated monitoring and searching of brand misuse in real time. This system uses more than 100 different data sources which are covering almost all the places where the intruders can place their weapons.



The toolbox is an expert system which main goal is to establish human - computer team capable of fighting with IP misuse. This system simply guides the user through the process of detection and response calling for action only if it is impossible to do all the things automatically. Simply like Adobe Illustrator for designers, our system is a powerful weapon for IP defenders.

IPLegist
Intellectual Property Protection Platform

HOW DOES IT WORK?

1. DETECTION

High-tech automated monitoring of more than 3,000,000 resources, tracking the appearance of platforms and their movements

DOMAIN NAMES	Domain names such as .RU, .РФ, .SU and thousands of others
MOBILE APP STORES	AppStore, Google Play, Windows Store, and others, including unofficial ones
SEARCH ENGINES	Yandex, Google, Bing and, if necessary, others
CONTEXTUAL ADVERTISING	Yandex.Direct, Google AdWords, targeted advertising on social media such as VK, Facebook, OK, Twitter
DATABASES OF PHISHING RESOURCES	Checks involve the use of more than 3,000 regular expressions and signature analysis
ONLINE CLASSIFIEDS AND MARKETPLACES	Avito, AliExpress, eBay, Amazon, Alibaba, Tmall, etc.
SOCIAL MEDIA AND OPINION LEADERS	VK, Facebook, OK, Instagram, Twitter, etc.
TELEGRAM CHANNELS	Bots used for monitoring Telegram channels relating to important events
DARK WEB	Monitoring of underground forums by experienced analysts

IPLegist
Intellectual Property Protection Platform

HOW DOES IT WORK?

2. ANALYSIS

Unique algorithms that help categorise the attack, assess how dangerous it is, and prioritise the response in order to reach a tangible result

SCORING OF FRAUDULENT RESOURCES

A comprehensive scoring system that analyses resources based on several indicators: domain registration date, cloud registry, use of certain types of CMS, and other criteria.

DETECTION OF COUNTERFEIT GOODS OFFERS

Automated identification of clearly counterfeited goods based on the content of the offer (based on facts such as price, product description, accompanying picture, article, etc.) and the resource/seller's affiliation with known fraudulent resources/offers.

COMPARISON WITH PARTNERS' WHITE LIST

To avoid blocking partner websites, in unusual cases a team of experienced analysts verify the links.

ASSESSMENT OF FINANCIAL LOSSES

Attacks are ranked based on potential financial losses, taking into account the conversion rate, the average purchase price, and traffic analysis. The most dangerous threats are handled as a priority.

EXTRACTION ON PHISHING KITS TO BLOCK THE ENTIRE PHISHING INFRASTRUCTURE

We extract the set of configuration files (phishing kits) from a given website, which allows us to identify the entire network of fraudulent resources and block access to the mailbox or resource to which user data is sent.

COLLECTION OF DIGITAL EVIDENCE

We collect data (screenshots, page source code, etc.) that are useful in the event of further investigations.

IPLegist
Intellectual Property Protection Platform

HOW DOES IT WORK?

3. RESPONSE

UNIQUE RESPONSE METHODOLOGY WITH SUCCESS RATE MORE THAN 95%

Fully automated and integrated with our systems.

INNOVATIVE TECHNOLOGIES

STRONG FOUNDATION

MODERATOR ACCOUNTS AND WELL-ESTABLISHED RELATIONS WITH MAJOR PLATFORMS

Threats are removed instantaneously through the interface/accelerated review of requests by administrators of major platforms.

AliExpress
Avito
ebay

A growing network of partners ready to help fight against scammers

RAPID RESPONSE IN 1,000+ DOMAIN ZONES

Direct links with domain name registrars and hosting providers, cooperation with response teams throughout the world.

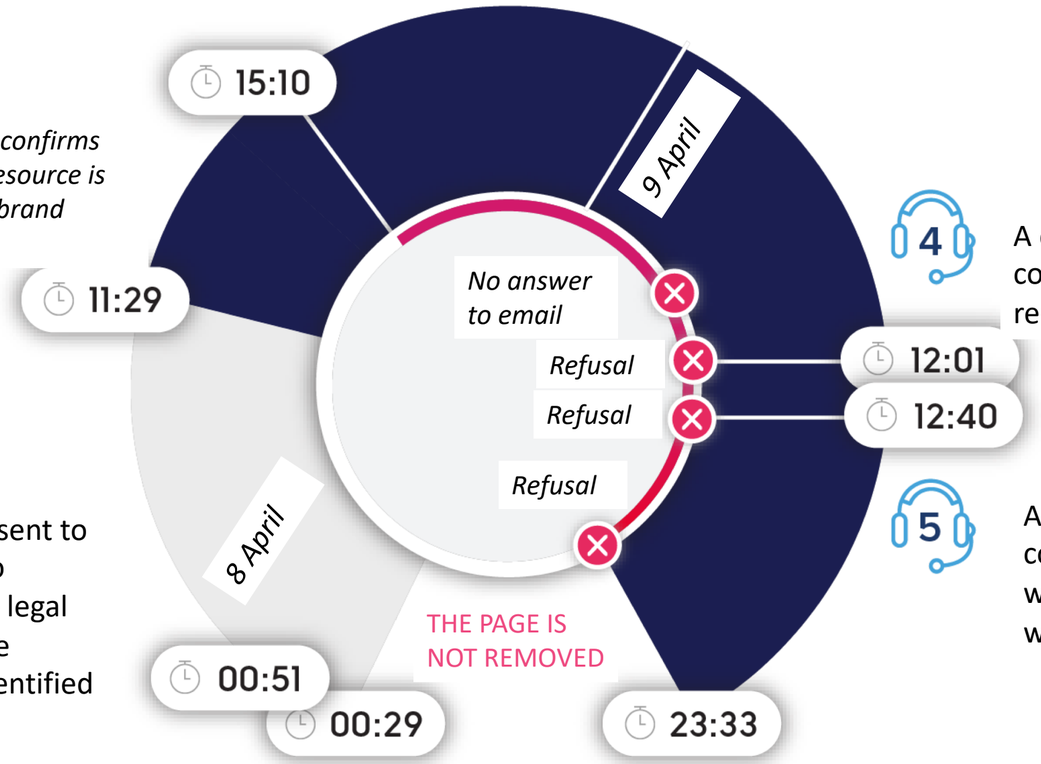
FIRST Improving Security Together
TI
CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
CERT AUTHORIZED TO USE CERT
IMPACT

Authorised member of international response team associations.

IPLegist
Intellectual Property Protection Platform

EXAMPLE TIMELINE OF THREAT REMOVAL

1 RESPONSE OUTLINE



3 An email is sent to the resource owner informing them about the rights violation

The client confirms that the resource is using the brand illegally

4 A call is made to the company director – the resource owner

2 An email is sent to the client to confirm the legal status of the resource identified

5 A call is made to the web design company that maintains the website and an email is sent with proof of the violation

1 The system identifies a resource that is likely to be using the client's brand illegally and collects the following evidence:

screenshot page source code

6 An email is sent to the domain name registrar and the hosting provider informing about the violation

IPLegist
Intellectual Property Protection Platform

EXAMPLE TIMELINE OF THREAT REMOVAL

2 RESPONSE OUTLINE

An email is sent to the national registrar informing about the cooperation with the domain name registrar to resolve the situation

Contact is made with top-level registrar to work together on remedying the violations

Procedure to verify registration details is initiated

Contact is made with other competent organisations and national CERTs to exert pressure on the offender

Contact is made with Internet network regulators (ICANN, OpenDNS, etc.)

THE PAGE IS REMOVED

As a result of comprehensive measures, the resource administrator makes contact at their own initiative and removes the illegal content from the resource

IPLegist
Intellectual Property Protection Platform

HIGH-TECH BRAND PROTECTION

ANTI-PIRACY

- Video content (films, TV shows, clips)
- Software (computer games)
- Books, newspapers, articles
- Music

ANTI-FRAUD

- Fake partnerships
- Illegal advertising
- Fake mobile apps
- Phishing and fraudulent websites
- Fake accounts and groups on social media

ANTI-COUNTERFEITING

- Illegal sale of goods on the Internet (online classifieds, groups on social media, messengers, websites, mobile apps)
- Grey import
- Breaches of partnership agreements

- Fashion & Retail
- Luxury brands
- Electronics
- Alcohol
- Cars
- Perfumes & Cosmetics
- Manufacturing
- Fast Moving Consumer Goods (FMCG)
- Children’s products
- Sporting goods
- Media industry

…

We return traffic

to official resources after blocking fraudulent websites and offers of counterfeit goods that intercept up to 50% of visitors.

We increase revenue

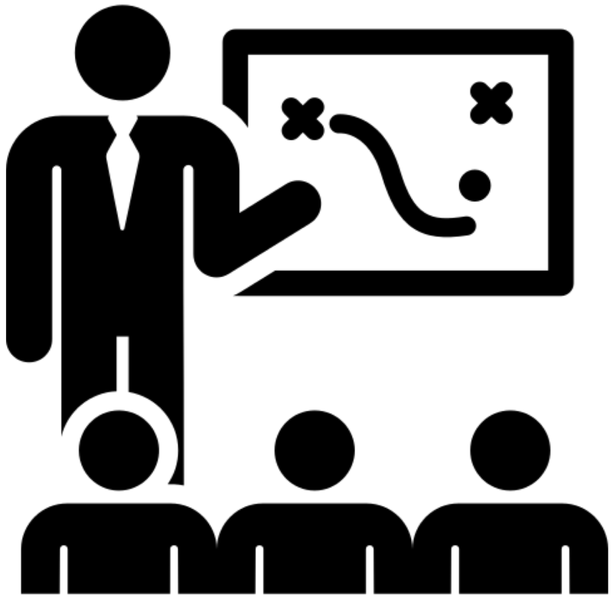
as a result of blocking sources of pirated content, decreasing the amount of counterfeit products available online, and reducing the damage resulting from illegal use of the brand.

We prevent losses

by detecting attacks and fraudulent activities at their early stages, thereby minimising reputation risks.

IPLegist
Intellectual Property Protection Platform

NEXT MILESTONES



- Fully functional version of the system, ready for usage. Finalizing UI & UX, last steps in the development of monitoring algorithms.
- Acquiring more clients in Europe.
- Registering new IP.
- Raising investment round for scaling.
- AI based tools for automated response PoC.

Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

Aleksandr Lazarenko

lazarenko@group-ib.com

www.group-ib.com info@group-ib.com twitter.com/groupib_gib

group-ib.com/blog +7 495 984 33 64 linkedin.com/organization/1382013