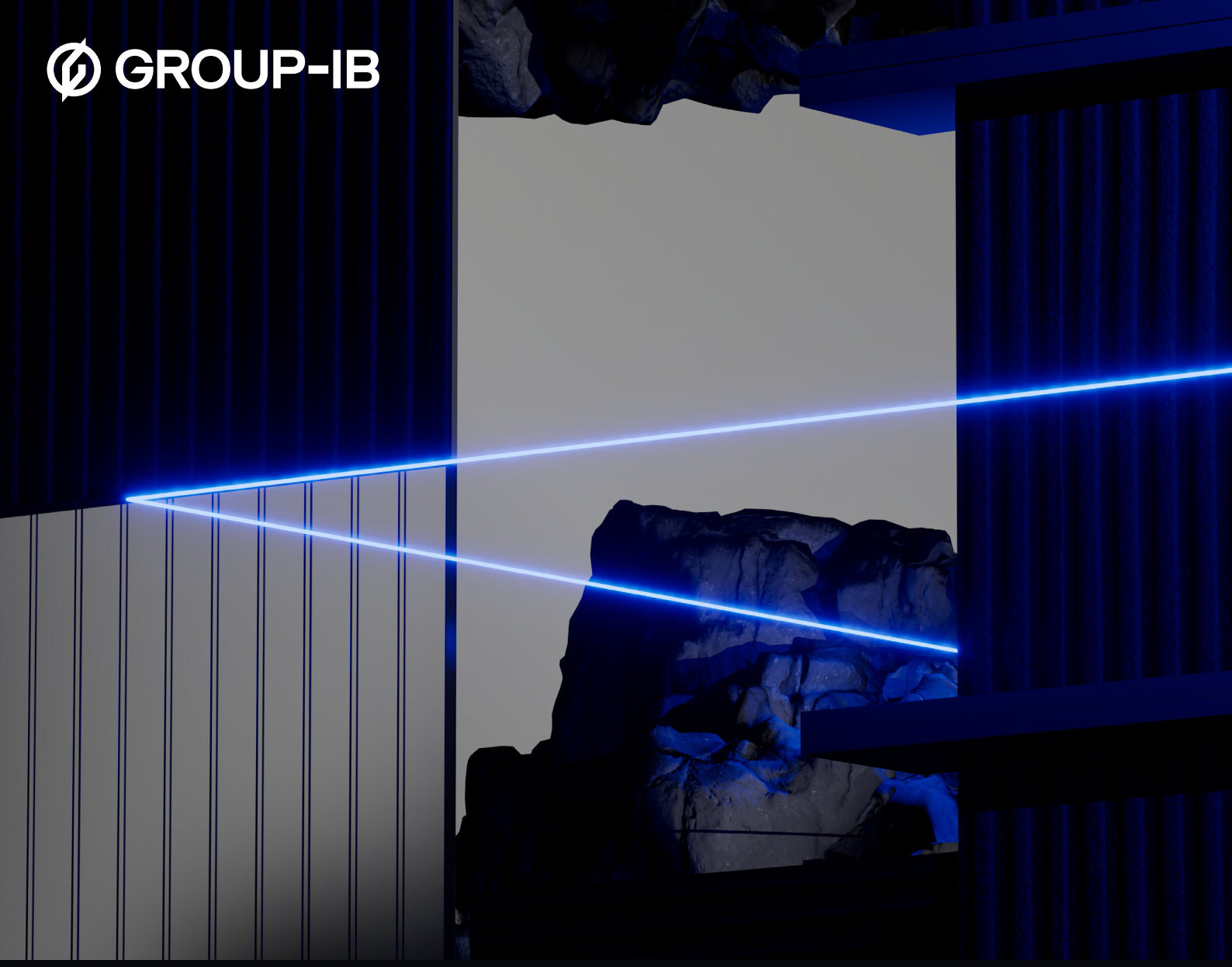
GROUP-IB



SUCCESS STORY

A DIGITAL WEALTH MANAGEMENT PLATFORM

Leverages Group-IB Digital Risk Protection to fight against brand abuse and prevent reputational and financial damage

What happened?

ABOUT OUR CUSTOMER

It is an Asia's leading digital wealth management platform for financial institutions.

The customer discovered there was a suspicious website imitating company's official website and contacted Group-IB to resolve the problem. This particular fraudulent website was made to steal money from visitors by offering them fake investments under company's brand.

They realised they needed urgent help from cyber security professionals specializing in digital risk and brand abuse protection, so they contacted Group-IB.

Just a tip of an iceberg

After the first analysis Group-IB identified that this suspicious resource is a part of a much larger infrastructure.

It appeared not to be a sole case: the resource owner is an advanced scammer with a distributed network of fraudulent websites attacking different brands.

How did Group-IB solve the issue?

“The potential damage estimation is no good news. According to Group-IB’s statistics, fraudulent website traffic can reach about 5 000 visitors per day. Average loss of every scammed user is 100-200 dollars.” —

KAMO BASENTSYAN,

Business Development Director (APAC), Group-IB Singapore

First of all, Group-IB researched the threat landscape for the customer as well as previous case details.

Group-IB Digital Risk Protection applies a complex approach to investigate and reveal the entire infrastructure of the attacker. We vetted all sources which may be used in fraud spreading and brand violation purposes:

- Search engine results
- Consonant domain names
- Social networks
- Classifieds
- Mobile application stores
- Image search
- Advertising

Analysis and attribution allowed us to understand that we faced a professional fraudster who was constantly creating such fraudulent websites and the resource our client signalized about was neither first nor last one.

We always provide our customers with:

Comprehensive information about Group-IB services	Details about current market climate	Different examples of use cases and figures	Recommendations on how enhance the cybersecurity strategy for their digital resources

Results

Analysis revealed:

100+
affiliates by registration data domain names

13
connections with other domains

Connection
with domain owner's personal avatar

As a result of this thorough landscape investigation, Group-IB revealed all potential risks and provided our customer with preventive recommendations. This helped to avoid the massive spread of fraudulent resources at an early stage.

Along with threat landscape research we also investigated the precedents. Group-IB checked the resource infrastructure if there are any affiliated resources aimed at the company. As a result, one more suspicious website was detected and taken down.

For investigation purposes we used Group-IB's technology — Graph.

Currently, Graph includes:

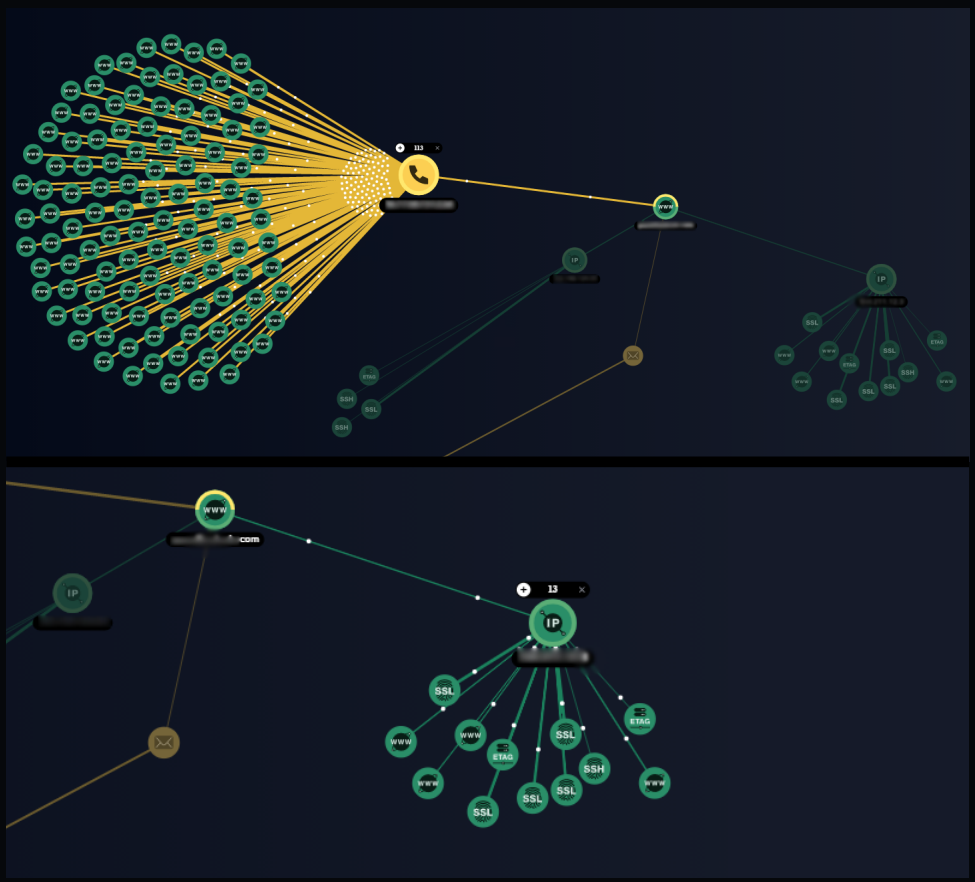
A DATABASE OF 1.4B DOMAINS
more than 577M second-level domain names

1B SSI CERTIFICATES

200M+ OF SSH KEYS

4.2B OF IP ADDRESSES

15 YEARS
history of all changes made in the web over last 15 years



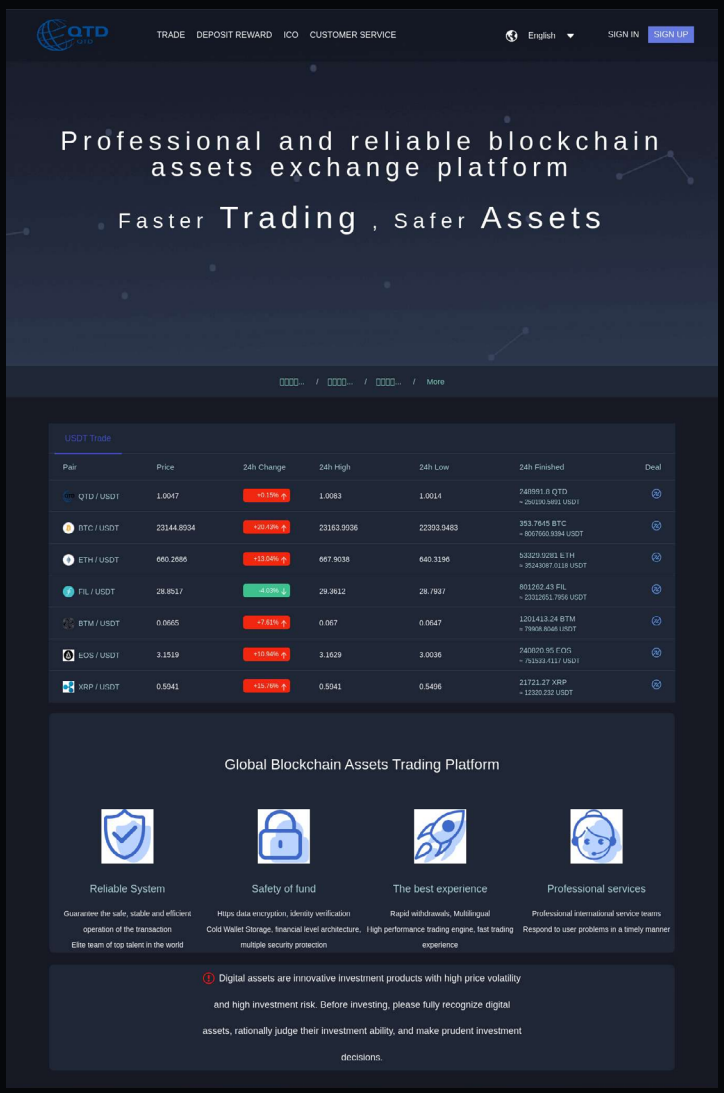
Domain owner used quite unique registration data which was captured by Graph. Deeper analysis revealed that the same data was recently used for registration of over 900 domains.

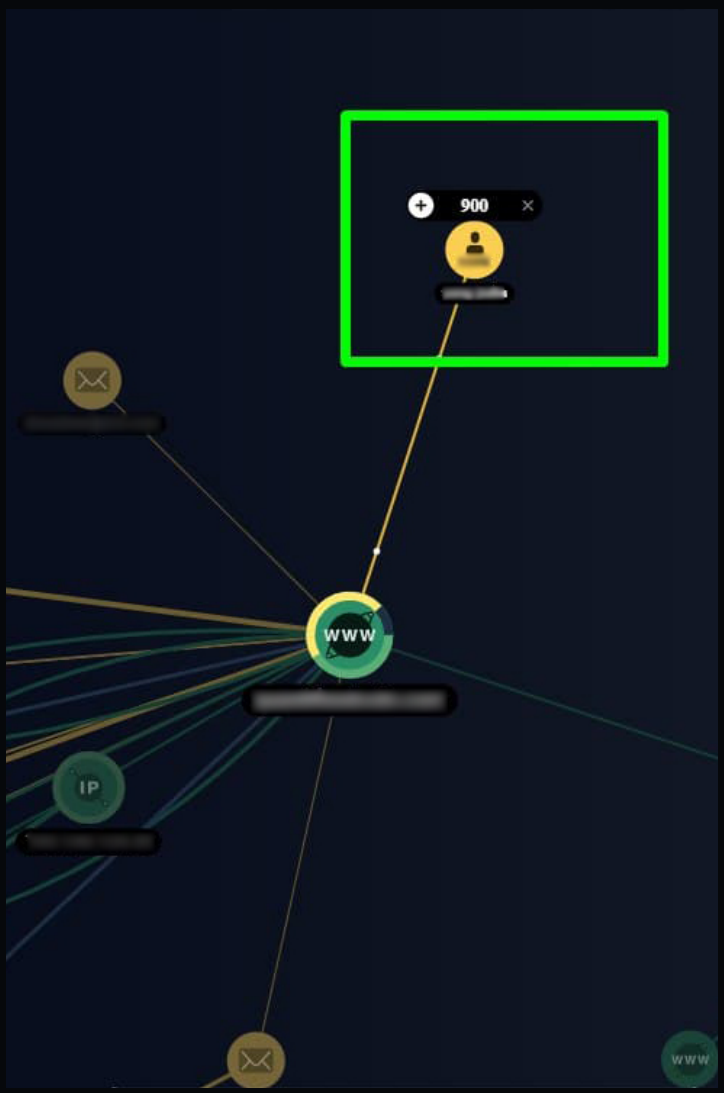
Stopping the activity of scammers

Those resources all belong to the same scammer but involve other brands or brandless scams.

Rapid and professional actions of Group-IB helped to stop attacks and protected client's brand from damage extension.

Following months of monitoring proved that the scam activity was completely stopped.





Current services from Group-IB include detection and response to any form of illegal brand or trademark usage, including social networks.

Group-IB's complex approach allows our customers to be assured that their digital reputation and users personal data are safely protected.

About Group-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,400+ Successful investigations of high-tech cybercrime cases	**300+** employees	**600+** enterprise customers	**60** countries
$1 bln saved by our client companies through our technologies	**#1*** Incident Response Retainer vendor	**120+** patents and applications	**7** Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

EUROPOL

AFRIPOL

Recognized by top industry experts

FORRESTER®

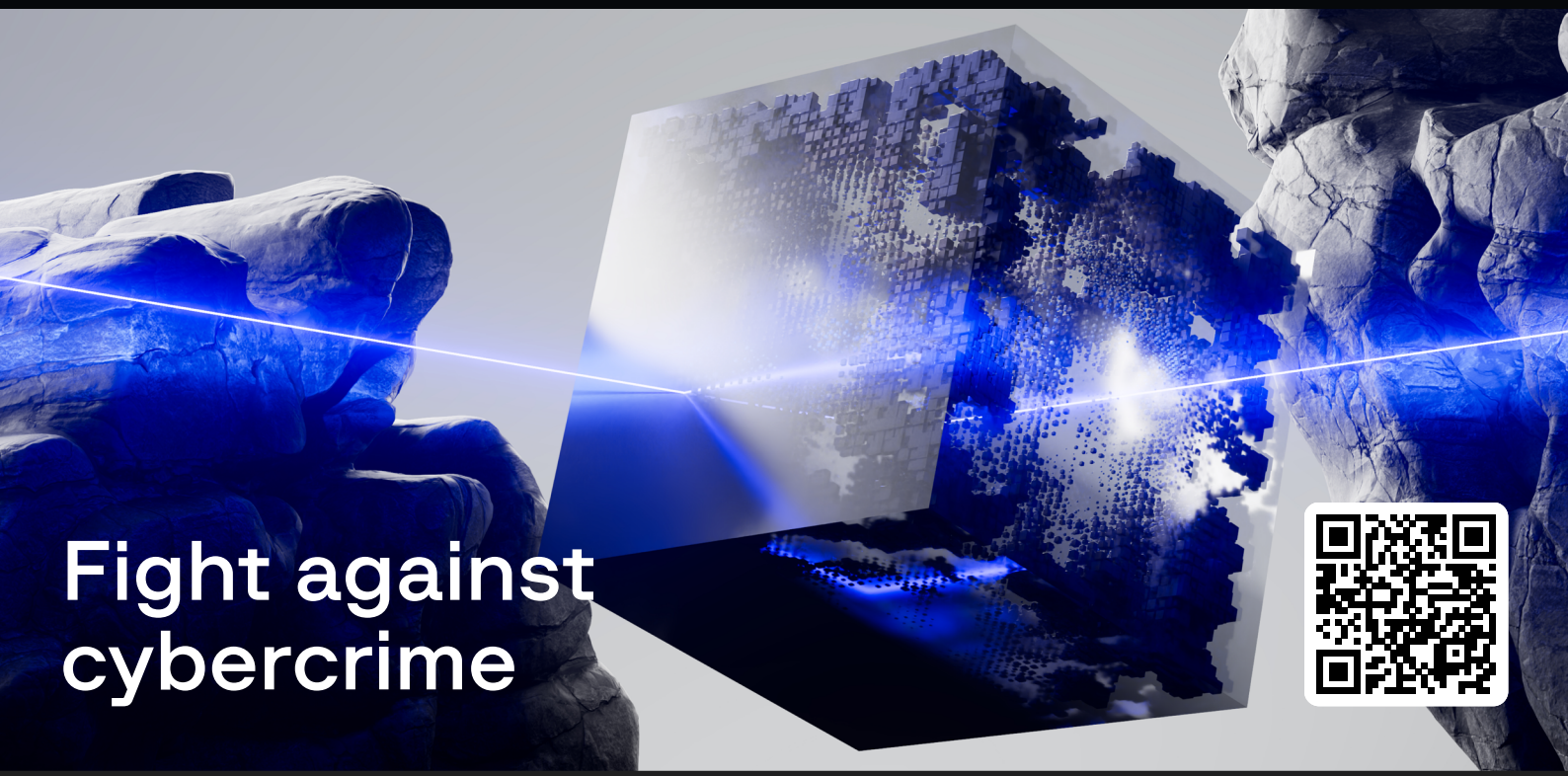
Aité Novarica

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN



Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785