SUCCESS STORY

GROUP-IB × YOUHODLER

Securing the future
of crypto lending

About YouHodler

INDUSTRY

Cryptofinance

LOCATION

Global

Member of the Crypto Valley Association

Member of the Blockchain Association of Financial Commission

YouHodler is a crypto-based platform where customers can exchange their cryptocurrency for fiat loans. The company understands that spending crypto assets today prevents cryptocurrency holders from gaining from any future growth in asset value, which means that investors who buy low need to hold onto their assets in order to benefit from selling high.

That is why YouHodler has made its mission to "help people stop passive holding and use crypto assets right here, right now."

To achieve this mission, YouHodler has dedicated itself to creating a highly inclusive service that supports BTC, BCH, BNB, ETH, LTC, XLM, XRP, DASH, HT, REP, and many other popular digital currencies and tokens.

YouHodler has unique expertise in commercial finance and FX/CFD trading; creating e-commerce and e-learning platforms; and working with blockchain and distributed ledger technology. The company combines the wisdom and practices from the world of traditional finance with the start-up spirit of the digital industry.

130,000+	**4.5 mln**	**Top 10 app**
New accounts opened in 2020	Unique visitors to YouHodler's website in 2020	Both in App Store and Google Play

Background

Pentest every 6 months

to ensure YouHodler's online platform is vulnerability-free

Creating a successful crypto lending service is only part of the job. YouHodler also makes great efforts to ensure that its online platform is as secure as possible, as it handles customers' money and sensitive information. A single vulnerability would not only compromise YouHodler's crypto storage but also customer loyalty and trust. Without either, YouHodler cannot exist.

The crypto lender, therefore, performs a penetration test every six months to check for vulnerabilities in its online platform. Given that the company's web portal hosts thousands of user accounts, YouHodler also has web application security assessments conducted for good measure.

In addition, YouHodler regularly evaluates its employees' awareness of modern social engineering tactics (i.e. phishing) to eliminate potential security incidents borne out of human error.

When it comes to choosing a vendor to fit the above needs, YouHodler looks at two main criteria: recommendations and the assessment plan. The lender consults with financial companies who share the same business model and security aims, collecting potential candidates from them. Then, YouHodler looks at the plans proposed by each company on the shortlist. Once an ideal plan is found, a final decision is made.

We received from Group-IB a pentest plan that met our criteria perfectly. This was one of the deciding factors in our decision. And we are happy we made it.

Renat Gafarov, CTO, YouHodler

Group-IB services

Group-IB's auditing team performed three tests for YouHodler: an External Penetration Test, Web Application Security Assessment, and Social Engineering Test.

External Penetration Test	Group-IB used the Black Box testing model (i.e. simulated the actions of an attacker who has no data about the external infrastructure). The following steps were taken:

1. Survey the IT infrastructure, including an analysis of IP addresses and network topology, and a scan of network perimeter nodes.
2. Identify vulnerabilities in applications and system-wide software.
3. Perform threat modeling, exploit vulnerabilities found, and simulate system attacks to see exactly how severe the vulnerability is.
4. Document and analyze results in a final report.

Web Application Security Assessment

Group-IB used the Grey Box testing model (i.e. simulated an attack where the attacker has access to the web portal). The following steps were taken:

1. Perform initial analysis of the application environment, and review publicly available information and resources to identify any sensitive information.
2. Identify vulnerabilities in the web application itself through manual discovery and application crawling.
3. Test the web application's business logic flaws.
4. Determine whether identified vulnerabilities can be exploited.
5. Document and analyze results in a final report.

Social Engineering Test

Group-IB experts evaluated employee awareness of social engineering attacks by sending phishing or active attachments to YouHodler employees. The following steps were taken:

1. Use OSINT to gather data about the company and obtain a list of users who will be targeted.
2. Develop a testing scenario and cover story, and agree on the testing tools (e.g. websites, executable files, text messages).
3. Test the tools' operability on the selected targets.
4. Carry out the testing scenario.
5. Document and analyze results in a final report.

The report for each test contained descriptions of all identified vulnerabilities, attack vectors, and operation methods, as well as recommendations on how to mitigate the vulnerabilities and weaknesses found.

Result

Revised access control policies and updated security rules for 4 teams

For YouHodler, Group-IB exceeded expectations. What first impressed the crypto lender was that Group-IB had immediately (and without preconditions) set up a communication channel, which facilitated frictionless and transparent cooperation throughout the assessment lifecycle.

But what impressed YouHodler the most was Group-IB's final report. The cybersecurity company revealed several previously undetected vulnerabilities, including those related to business logic. With the help of Group-IB's recommendations, the lender was able to remedy all vulnerabilities within a short period of time. The report also led to YouHodler updating their security rules for four teams and revising their access control policy for all personal data storage.

Given the exceptional work conducted, YouHodler expects to have more frequent cooperation with Group-IB in the future. Apart from penetration testing, the lender wants to explore other auditing services that Group-IB provides, all in the hopes of creating the most reliable and secure lending platform for its customers.

Working with Group-IB was a great experience. Their experts provided fast and transparent communication, and their hard work resulted in a clear, thorough analysis that helped us to improve our company for the better.

Renat Gafarov, CTO, YouHodler

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