GROUP-IB

fawry

SUCCESS STORY

GROUP-IB × FAWRY

How Group-IB helped Egypt's largest e-payment provider avert ransomware threat

How did Group-IB provide expertise to avert ransomware?

Industry	Financial Services, E-payments
Size	5,001-10,000 employees
Founded	2008
Country of origin	Egypt

Digital Forensics and Incident Response (DFIR) Team

Group-IB DFIR experts are primed to intervene to block and mitigate attacks and eliminate potential harm immediately.

In the case of ransomware, where each moment counts, our Forensics and Incident Response analysts prompt assistance to Fawry in retracing and evidencing the attack, and the adversary behind it became critical in minimizing damage.

Group-IB Threat Intelligence

(Group-IB Threat Intelligence has tracked LockBit since the group's inception)

Group-IB **Threat Intelligence** was enabled as an advanced monitoring and intelligence tool to look into the attack trails and recreate the MITRE ATT&CK® timeline.

Group-IB Managed Extended Detection and Response (MXDR)

Group-IB MXDR technology was enabled to perform run-time and historical analysis of the attack through live telemetry and forensic data collection covering all endpoints in the testing environment.

Introduction

Electronic payments surely bring convenient, time-saving, and seamless transactions, but what one might see as a three-click simple process involves a whole other level of complex infrastructure to make one transaction happen. It is a multi-component process involving website/ application interfaces, payment gateways, processors, and networks behind the scenes - each can have exposures that cybercriminals could exploit, putting your businesses' and your customers' faith in the entire system to the test.

This emphasizes the importance of maintaining robust security measures across all e-payment and financial services, starting from the first line of infrastructure code, especially when cyber adversaries are increasingly motivated to exploit any vulnerabilities for potential intrusions and attacks.

It is standard practice to segregate development and **testing environments** from production ones. In the case of Fawry, this isolation was even physical due to its high-security, high-reliability systems. However, despite that, cybercriminals might still find ways to intrude into your testing environment, potentially causing disruptions.

Such was an impasse experienced by Egypt's largest e-payment service provider - Fawry. LockBit (2023's most prominent ransomware-as-a-service group with 1,079 posts on its DLS (24% of the annual total as per Hi-Tech Crime Trends Report 23/24) tapped into their data inventory to exfiltrate information, encrypt files, and demand ransom.

Beyond mitigating the crisis, **there were associated situational challenges. As a $2 billion company, Fawry was extra cautious in ensuring unhindered and continued operations**. Group-IB not only assisted Fawry in navigating through this difficult period but also provided tangible support in helping the company gauge the crisis deeply and share credible communication about its impact on its extensive user base.

Comprehensive investigation and analysis of Fawry's cybersecurity infrastructure

The investigation and threat interdiction began after a post was published on the Lockbit threat cluster on their Data Leak Site (hereinafter – DLS) on November 8th, 2023.

8th November, 2023

LockBit published a post about the ransomware attack on Fawry.

9th November, 2023

On the first weekend of the month, Fawry contacted Group-IB. Our DFIR (Digital Forensics and Incident Response) team immediately engaged in incident response engagement, providing uninterrupted support.

10th November, 2023

Fawry immediately took containment measures and issued an announcement that its live production environment had not been breached. The Group-IB team was engaged to validate Fawry's findings and identify the complete scope of the attack.

12th November, 2023

Over the course of three days, Group-IB's proprietary technologies were deployed across 100% of Fawry's server infrastructure.

12th - 23rd November, 2023

Group-IB worked on the following engagement objectives:

- Identifying the attack's root cause and concrete timeline to understand the threat actor's TTPs used and to prevent future incidents.
- Ensuring no active threats or attack tools were present on Fawry's infrastructure and issuing a clean bill for cyber health.
- Identifying any weaknesses in Fawry's network that attackers could exploit.
- Providing PR and communication support during and after the incident for all stakeholders.

23rd November, 2023

Completion of the network cleanup and analysis of Fawry's production environment.

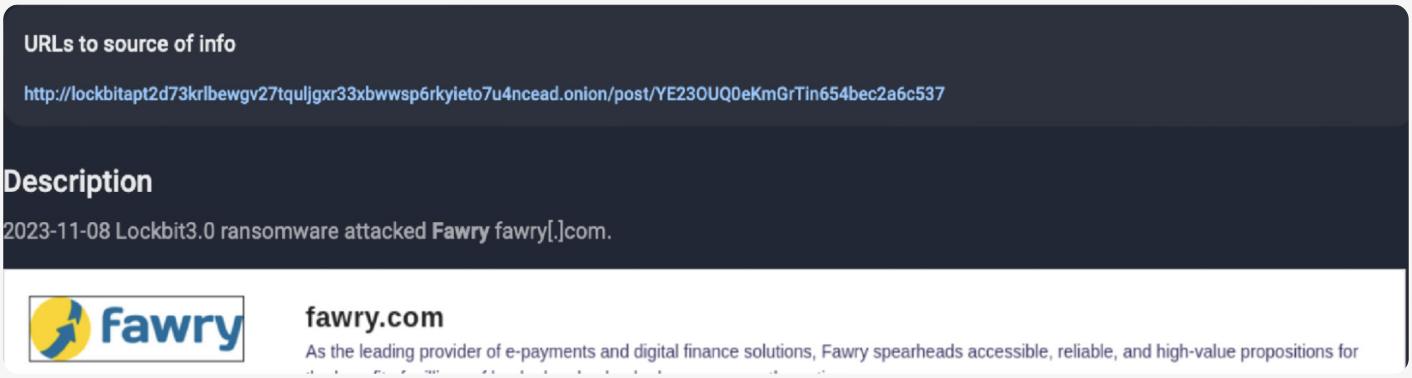
24th November, 2023

Group-IB issued a full report confirming the completion of network cleanup and validating that the threat actor did not access, collect, or exfiltrate any production segment, payment information, or customer data.

26th November, 2023

Both Fawry and Group-IB issued separate press releases confirming the successful collaboration.

LockBit claimed a successful ransomware attack on Fawry, encrypting Fawry's testing environment infrastructure and exfiltrating some portion of the data. These claims weren't made without substance and were supported by screenshot proof of several Personal Identifiable Information (PII) entries of Fawry's customers.



URLs to source of info

http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion/post/YE23OUQ0eKmGrTin654bec2a6c537

Description

2023-11-08 Lockbit3.0 ransomware attacked **Fawry** fawry[.]com.

fawry.com

As the leading provider of e-payments and digital finance solutions, Fawry spearheads accessible, reliable, and high-value propositions for

Figure 1.
Lockbit DLS post about attack on fawry

Fawry was given a 20-day ultimatum to pay the ransom, with the deadline being November 28th, 2023. To prevent the situation from escalating into a full-blown crisis, Fawry sought the help of Group-IB experts. Group-IB quickly initiated the process of collecting evidence of the attack and conducting an in-depth technical analysis, including the scale and scope of the attack.

إلى أن وصلنا إلى التقرير النهائي
والذي أعلنا فيه

4:23 / 49:40 • ما حقيقة مشكلة اختراق "فوري" التي حدثت في مصر مؤخرا؟

الرئيس التنفيذي لشركة فوري أشرف صبري - ضيفي مع معتز الدمرداش

Asharq News - الشرق للأخبار
1.15M subscribers

Figure 2. Ashraf Sabry - Chief Executive Officer at Fawry talking about collaboration with Group-IB to help mitigate the cyber threat.

Major Pain Points that Group-IB and Fawry Jointly Overcame:

1. Evaluating and confirming if Fawry's production segment remained unaffected during the incident.
2. Verifying the safety of Fawry's production segment for third-party use.
3. Ensuring that Fawry's Testing and User Acceptance Testing (UAT) (pre-production) segments are free from the Lockbit threat cluster.
4. Developing MITRE ATT&CK® timeline of the Lockbit ransomware attack to provide a comprehensive view of the incident, including root cause analysis, persistence, compromised credentials, scoping of leaked data, and impacted assets.

Solutions offered

1. Complete coverage of Fawry's production and testing environments with Group-IB Extended Detection and Response (concurrently enabled with Fawry's other security controls).

100%	100%
Fawry's production environment covered	Fawry's UAT + Testing environment covered

2. Contextualize the cyber-attack kill chain, implied Tactics, Techniques, and Procedures (TTP) of Lockbit threat cluster affiliates using Group-IB Threat Intelligence and insights from previous Fawry incident investigations.
3. Continuously monitor Fawry's infrastructure using Group-IB MXDR technology, detecting malicious events through manual and automatic approaches.
4. Perform point-in-time forensic data collection from all endpoints to ensure:
   a. Proper scoping of the cybersecurity incident, identifying all endpoints with files and folders encrypted by ransomware.
   b. Identification of Lockbit's TTPs and IOCs in the intrusion to Fawry.
   c. Accurate root cause analysis of the attack.
5. Conclude the analysis and provide a clear statement to Fawry and relevant authorities.

Group-IB Digital Forensics and Incident Response Team's (DFIR) Findings

Offering Fawry An Official Clean Bill of Cyber Health

When the report was written in November 2023, the following conclusions were made and submitted by Group-IB.

- Group-IB confirmed that Fawry's Production environment was not affected by the Lockbit ransomware attack.
- Group-IB confirmed that there was no current presence of Lockbit's threat cluster in Fawry's Production, UAT, and Testing systems
- Group-IB finalized the technical analysis of the Lockbit ransomware attack.
- Group-IB continued to provide post-incident services through ongoing coverage with our Extended Detection and Response (XDR) tool and threat-hunting services, ensuring no further risk persistence or disruptions occur in Fawry's network.

Fawry, with Group-IB's comprehensive support and technical expertise, evidenced the optimum level of cybersecurity maintained for their testing and live operational environments. To maintain transparency and long-standing trust in the brand, this was officially communicated to the stakeholders and the public through a **press release**.

Conclusion

This collaboration study showcases a strong partnership that resulted in timely and thorough ransomware attack analysis and complete network cleanup, solidifying security for the e-payment giant. Group-IB experts utilized the patented advanced monitoring, intelligence, and detection technologies and investigative expertise to provide comprehensive insights into the infrastructure of the leading e-payment business, identifying potential attack vectors exploited by the ransomware authors.

Group-IB will continue to actively monitor Fawry's systems and assess the necessity for any additional security measures as needed. Furthermore, Fawry maintains a proactive approach to ensure robust cybersecurity across its entire infrastructure. The company engages with global consultancy firms to review its governance and risk assessment policies, enhancing existing frameworks to align with the utmost standards.

Unprecedented challenges like ransomware require expert cybersecurity guidance

If you suspect or are experiencing a ransomware attack, contact us through Group-IB's immediate helpline: response@cert-gib.com. To build an end-to-end protection strategy against ransomware and other advanced threats, visit our **dedicated page** or give our experts a nudge **here**.

About Fawry

Founded in 2008, Fawry is the largest e-payment platform in Egypt, serving the banked and unbanked population. Fawry's primary services include enabling electronic bill payments, mobile top-ups, and provisions for millions of Egyptian users. Other digital services also include e-ticketing, cable TV, and a variety of other services. Through its peer-to-peer model, Fawry is enabling corporates and SMEs to accept electronic payments through a number of platforms, including websites, mobile phones, and POSs. With a network of 36 member banks, its mobile platform, and 280 thousand agents, Fawry processes more than 3 million transactions per day, serving an estimated customer base of 49 million users monthly

About Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its technological capabilities to defend businesses and citizens and support law enforcement operations. Group-IB's **Unified Risk Platform (URP)** underpins its conviction to build a secure and trusted cyber environment by utilizing intelligence-driven technology and agile expertise that completely detects and defends against all nuances of digital crime. The platform proactively protects organizations' critical infrastructure from sophisticated attacks while continuously analyzing potentially dangerous behavior all over their network.

About Group-IB

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

1,550+	Successful investigations of high-tech cybercrime cases
400+	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
8	Unique Digital Crime Resistance Centers

* According to Cybersecurity Excellence Awards

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- FORRESTER®
- AiteNovarica
- 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