GROUP-IB

CASE STUDY

RANSOMWARE

Special needs school recovers infrastructure and improves in-house capabilities with Group-IB Incident Response

Introduction

Industry	Education & Healthcare
Activities	Educational services for children with special needs
Region	Europe
Products and services	Group-IB Incident Response, Group-IB Managed Extended Detection and Response (MXDR)

Ransomware remains the top threat in Europe. Group-IB's research revealed a **52%** year-on-year growth for **ransomware attacks** in 2023, yet many incidents are not included in statistics because they go unreported. Schools are an attractive target for ransomware operators for a few reasons. They store valuable personal and financial information as well as their own confidential research and intellectual property. At the same time, they can rarely afford to invest a huge amount in defense solutions, regular security check-ups, or large dedicated teams of cybersecurity professionals.

Educational organizations have a great deal of responsibility towards their clients — the pupils and their parents. Ransomware attacks can have consequences such as theft of sensitive data, operational disruption due to lost access to systems, financial repercussions, and reputational damage. In the face of immense pressure and the high risk of sensitive information being stolen or leaked online, such organizations often choose to negotiate with criminals and ultimately pay the ransom.

What's more, following initial breaches, threat actors often create additional points of entry within the infrastructure. This means that even if an organization manages to contain a single incident, it could face repeated attacks in the future. In such cases, it is essential to turn to **professional incident response teams** with solid skills, advanced forensic tools, and extensive experience in digital forensics. Only such professionals can ensure that your digital assets are safe to use.

Learn effective strategies and best practices for preventing and responding to ransomware attacks.

Solutions for Ransomware Protection ↗

Challenge

Mitigating the consequences of a ransomware attack

A school for children with chronic illnesses, physical disabilities and learning difficulties experienced a ransomware attack and their files were held hostage. In this instance, the risk was double: in addition to compromising the family information usually stored by educational organizations, the attack could have affected information about the health conditions of the pupils.

A threat group known as HsHarada exploited a ProxyShell vulnerability, escalated privileges, disabled Windows Defender, and installed Cobalt Strike for reconnaissance purposes. Next, the threat actor deployed ransomware and encrypted several servers but left no evidence of data exfiltration.

Swift intervention by the school's IT team helped to limit the damage. Thankfully, the team was able to restore the affected data from backups. However, the school decided to hire Group-IB experts to investigate and remediate the attack and to ensure that all traces of ransomware would be removed.

Initial pain points:

- Stretched IT team with limited resources and tools
- Lack of expertise and experience in countering complex cyberattacks
- Insufficient scope of past security assessments
- High risk of further attacks
- Lack of full control over the infrastructure
- Outdated security strategy and practices
- Lack of visibility into the organization's gaps, misconfigurations, and vulnerabilities

Solution of choice

Group-IB Incident Response: seasoned experts and stellar technologies

Group-IB's Incident Response service has a 20-year proven track record in analyzing and responding to attacks of any complexity, all over the world. Our distributed team of certified experts can perform a quick but thorough analysis to help you contain, remediate, and recover from serious attacks.

Group-IB experts leverage the full stack of in-house digital forensics, threat intelligence and malware analysis tools to check the entire infrastructure, collect digital evidence, and attribute threats to specific actors. They reconstruct the attack lifecycle and retrace the adversary to stop the ongoing campaign and prevent future attempts. Our round-the-clock CERT-GIB team monitors your company's infrastructure for two weeks after incident response so that your IT team can implement all our recommendations while staying protected.

Effective incident response gives organizations more than just the remedy to one incident. It ensures visibility into weaknesses in affected systems and the entire infrastructure, which ultimately helps to enhance your organization's prevention and detection capabilities.

Be prepared with the fastest incident response. One agreement covering all proactive and reactive cybersecurity services needed.

Group-IB Incident Response Retainer ↗

Outcomes

Second attack stopped, systems updated and prepared for the unexpected

Group-IB's Incident Response team was quick to support the school. The team gathered essential data both remotely and onsite to speed up incident response. At the same time, the experts deployed Group-IB Managed XDR to monitor the infrastructure. This approach helped recover the entire kill chain, attribute the attack to a specific group, and block the command-and-control (C&C) servers involved in the incident. Group-IB experts removed the ransomware from the systems and eliminated all points of access that the threat actors could use.

Shortly after Group-IB specialists completed their analysis and provided recommendations for preventative measures, MXDR detected a second intrusion attempt by the same group, exploiting the same vulnerability. The threat actors were once again using Cobalt Strike and similar tactics, techniques, and procedures (TTPs). The attackers intended to cause more disruption, which could have led to systems being corrupted and sensitive data being stolen or encrypted. Group-IB Managed XDR promptly detected and thwarted the attack before any damage could happen.

After the second incident, Group-IB worked closely with the school's IT team to reconfigure the existing security systems. The Group-IB team delivered a detailed report with key expert findings, the root causes of the incident, and concrete steps to avoid similar ransomware attacks in the future. Our specialists also provided clear recommendations on how to improve the organization's overall security architecture and make it more resilient to cyberthreats.

Success highlights

Quick incident containment and remediation

Detailed recommendations and actionable insights

Clean and safe infrastructure

Organization prepared to tackle ransomware attacks

Properly configured security controls

Customer data secured

Conclusion

> Group-IB specialists demonstrated exceptional expertise and professionalism in their handling of the situation. Their clear communication, effective solutions, and insightful recommendations not only resolved the immediate issue but also equipped our school with the knowledge to enhance our cybersecurity measures. We highly recommend their help to any institution seeking robust and reliable cybersecurity solutions.
>
> **Information Security Manager at the school**

When ransomware strikes, every minute counts. Group-IB's Incident Response team was just on time to stop the incident, investigate the reasons behind it, and prevent severe consequences. In line with our social mission and commitment to support the community, Group-IB provided Managed Extended Detection and Response (Managed XDR) to the school at no cost. With its infrastructure upgraded, our recommendations put into practice, and Managed XDR's advanced threat monitoring capabilities at hand, the school is now ready to prevent and stop future attacks.

Emerge ever-stronger from any cybersecurity challenge. Strengthen your security posture and arm yourself fully against ransomware attacks with Group-IB's Incident Response team.

Learn more ↗