











10 Recommendations

for preventing ransomware attacks



-  Use VPN whenever accessing servers through RDP.
-  If it is not possible to use VPN, implement multi-factor authentication.
-  Block accounts after a certain number of failed login attempts within a short period of time.
-  Ensure that the password of the account used for access via RDP is complex and change it regularly.
-  Use NLA (Network Level Authentication) for RDP connections.
-  Restrict the list of IP addresses that can be used to make external RDP connections.
-  Install anti-spam and anti-phishing filters.
-  Regularly update anti-virus protection and audit the work logs of your protection software.
-  Implement a sandbox solution to detect malware not detected by antivirus software.
-  Perform timely updates of operating systems and application software.

Response to ransomware is extremely important



Access to the data on a device infected with ransomware cannot be restored without decryption tools, and it is not recommended to pay ransom to the attackers.

Group-IB experts prepare a detailed report describing the incident as well as a set of recommendations for improving infrastructure security. This minimizes the risk of similar incidents in the future.

Professional response to ransomware allows you to:

- Minimize damage
- Clean the infrastructure in order to prevent similar incidents in the future, including detection of "sleeping" backdoors
- Gather all necessary information for creating a list of Indicators of Compromise
- Collect an evidence base, as well as information necessary for the investigation
- Get recommendations on enhancing information security level of infrastructure and personnel

The Group-IB team would be more than happy to support your business by offering the following:

- Remote Incident Response service.
- Two additional free months for yearly subscription to the Incident Response Retainer service. [Learn more](#)

Contact us to learn more about the services: internationalsales@group-ib.com

Experiencing a breach?

24/7 incident response
hotline



Get help now:

- call us on **+65 3159-4398**
- email us at response@cert-gib.com
- fill out our incident [response form](#)