



Ransomware Incident Response Negotiation and Recovery

You've been hit with ransomware. What's *your* plan?

Organizations often struggle to deal with the aftermath of a ransomware attack. It can take days to contain the incident and analyze what systems and servers have been impacted. Then there are numerous questions to consider, such as:

- Do you pay the ransom?
- How do you acquire cryptocurrency?
- How do you decrypt the files once we've paid?
- Do you have confidence interacting with bad actors?

Rocus Networks' support team will mobilize to handle any ransomware incident, including cyber extortion, hacker communications, cryptocurrency movement, and file decryption and recovery. Rocus Networks is equipped with the expertise and latest tools to ensure recovery time and costs are minimized.

Here's *our* plan.



1. **Diagnosis.** We conduct attacker and malware scenario analyses to identify what computers, servers, and systems have been compromised. We also work to help contain the malware and protect the other parts of your organization.
2. **Negotiations & Decisions.** We work with you to analyze existing back-ups and network architecture. We also handle communications with the attackers, including negotiation of the ransom amount. We help you decide if paying the ransom is necessary and begin working with you to rebuild and restore your systems if it is not.
3. **Cryptocurrency Acquisition.** We handle the configuration of cryptocurrency wallets and acquisition of cryptocurrency to eliminate this headache for you.
4. **Disbursement.** We process the actual disbursement of funds and follow-up communications should you choose to pay. Many organizations use unsecure communication methods when dealing with attackers, creating additional vulnerabilities. We know how to mitigate that risk.
5. **File Decryption.** There is no "easy button" for file decryption. When a ransom has been paid, our team will work to analyze the decryption tool provided and ensure the network is configured so that nothing interferes with the decryption process to cause further damage to files.

In 2019, a ransomware incident will strike an organization about every 14 seconds.* We are here to help deal with this unsettling, confusing process and get your organization back up and running as quickly as possible.

Contact Rocus Networks at the first sign of a ransomware attack.

(800) 349-0976 | info@roculusnetworks.com | roculusnetworks.com