Steps to Take When Faced with a Ransomware Attack

Luis Simonet

NXTsoft CISO

What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user’s data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates data, or ransomware in conjunction with other malware that does so.

Despite rising awareness of the ransomware risk, this cyber security threat continues to wreak havoc on organizations of all types, disrupting normal business operations. The fact is while companies may now be more aware of the risks they are facing, cyber-criminals continue to stay a step ahead identifying newer vulnerabilities to exploit and finding more effective strategies for getting what they want. That is why we often say it’s not so much a matter of if you will be attacked, but rather when.

How To Prepare for a Ransomware Attack

Realizing your business is a victim to a ransomware attack is stressful. Nevertheless, the first thing to do is try to react calmly.

First and foremost, having an incident response plan directing employees on what to do if they come face to face with ransomware can exponentially increase an organization's resilience to ransomware attacks.

What to do prior to the attack:

- Conduct a Business Impact Analysis (BIA)
  In order to prepare for an attack, organizations need to conduct a BIA (business impact analysis) to determine the RTO (recovery time objective), RPO (recovery point objective) and criticality of your data and implement a back-up strategy to meet those determined requirements.
- Create, Maintain and test the Incident Response Plan.
- Perform Backups
  Backups need to be either created offline and/or stored where they can’t be directly reached by devices likely to be infected. Ransomware goes after backup files on network shares, it even deletes shadow copies on the workstation to prevent restoration.

After the Attack

What to do post attack

- Identify infected devices.
- Disconnect computer/server from the network. Do not power-off
- Take a picture of the ransom note. Authorities may need it later.
- Inform employees and any other appropriate organization
- Determine what you’re dealing with. Use the information in the ransom note to help you research the situation.
- detect and conduct an initial analysis of the ransomware;
  - determine the scope of the incident to identify what networks, systems, or applications are affected;
  - determine the origination of the incident (who/what/where/when);
  - determine whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment; and
  - determine how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited).
  - Determine what kind of ransomware it is

What to do post attack

- contain the impact and propagation of the ransomware;
- eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- recover from the ransomware attack by restoring/decrypting (if available) data lost during the attack and returning to “business as usual” operations; and
- conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents. If applicable report to authorities

Questions