ORCA CO., LTD.
3F X's Bldg., 26-22, Higashi-Ohi 5chome, Shinagawa-ku Tokyo, Japan
TEL:81-3-3471-8898 FAX:81-3-3471-8899 E-mail: systemdiv@orcajpn.co.jp

ORCA REPORT: Countermeasures Against Ransomware Attacks to Vessel

・Forewords

Recently, it has been reported that KADOKAWA's server was attacked by ransomware (ransom-demanding malware). This attack resulted in the leakage of most of the information on the company's business server and caused operational disruptions. In 2024 alone, major companies such as Nippon Life Insurance Company, KUBOTA, and KUMON have suffered personal information leaks due to ransomware attacks.

Ransomware attacks are spreading worldwide. Although there have been no reports of ransomware attacks on vessels yet, it's a solid fact that taking precautions and countermeasures against such attacks is essential.

For your reference, this document summarizes countermeasures against ransomware attacks in shipboard networks.

・Conclusion

Main points of countermeasures against ransomware:

1) There's no one single solution that guarantees 100% security.
2) To reduce the possibility of an attack, the implement a combination of antivirus, monitoring systems, network design, and user education is necessary.
3) To minimize damage if an attack occurs, it is crucial to identify and modify the operation of critical data, as well as to perform regular backups.

・What is *Ransomware*?

Ransomware stands for "ransom-demanding malware". When this malicious software is executed, it not only encrypts data within the network but may also send it externally.

Once infected, the data within the network becomes unusable, causing operational disruptions. Decrypting the data requires a code key and the ransomware attacker would demand money (ransom) in exchange for this key.

If the data includes sensitive information such as personal or corporate confidential information, the attacker may also threaten to leak it in order to get ransom from victims.

・The Attack Path

Ransomware can invade through various channels such as email, internet downloads, VPN, and user-installed software. Recently, VPN vulnerability has been reported as a common path of attack.

・Challenge in Defense

Different from typical computer viruses, ransomware is a "customized program" targeting specific networks, making it difficult to detect by the antivirus programs that rely on definitions of known malwares. Moreover, even the antivirus programs that use algorithm techniques cannot guarantee detection. Many ransomware attackers would also maliciously lead users to grant permissions to execute the malware, making all accessible data vulnerable. While some monitoring systems can detect and warn against ransomware activities, by the time the warning is issued, it turns out too late as significant damages may have already occurred.

・Types of Information Damage

The following shows the 3 major types of damage caused by ransomware:

1) Availability Damage
   Encrypted data cannot be accessed when needed, resulting in disruption in operations. For instance, imagine the chaos situation when finding you cannot access the past SMS record right before PSC.
2) Integrity Damage
   Ransomware may not only encrypt but also modify or delete data, causing the existing data unreliable for use. This is similar to the damage caused in type (1).
3) Confidentiality Damage
   Data can be leaked once infected. If the data contains corporate confidential information, the loss of corporate know-how could directly cause damage to the company, leaking personal or related parties' information may also result in compensation liability.

・What to Do if Infected

Avoiding contacting and paying ransom to attackers is needless to say, as there is no guarantee of data recovery and, in some countries, paying ransom may even be considered funding terrorism.

According to the SMS manual, please assemble an emergency response team, gather information and seek expert advice. Public disclosure may be necessary in some cases.

・Preventive Measures Against Potential Attacks

While preventing ransomware is extremely challenging., the following general measures should be implemented correctly in order to reduce the risks.

Use of Email	Avoid whitelisting Email domains as it can create entry points for attacks.
Anti-Virus Use and Updates	Making it possible to block the already-known ransomware.
OS and Software Updates	Patching security holes in OS can reduce risks in potential attacks.
Network Segregation	Separate internal networks by function to limit damage from VPN breaches.
User Education	Running software without companies' approval can cause unexpected incidents. As all malware comes in the form of software program, avoid running unapproved software can avoid damages. Therefore, user education is of utmost importance.

・Measures of Minimizing Damages

1) Confidentiality Measures

As its name implies, ransomware demands ransom from victims, therefore the more confidential the data is in the network, the more likely to be threatened for ransom. Therefore, conducting a risk assessment on the data confidentiality on each vessel become necessary.

Generally, vessels do not hold highly confidential data that would lead to compensational result. However, still need to be cautious with related party's confidential information. Understand the nature of each type of data and take effective countermeasures accordingly.

Low Confidentiality Data	Understand the content and accept the risk of leakage.
・High Confidentiality Data ・Data Subject to Compensation Liability If Leaked	Rather than a shared folder that can be accessed by everyone, use personal folders or physically separated drive to prevent potential leakage. Additionally, compress data in ZIP files with password can reduce the risk if leaked. DO NOT store passwords on the server.

2) Integrity and Availability Measures

Regular backups in system can ensure safe recovery in most cases. Discard the data that has been encrypted by attackers, and continue normal operation by using the backup data.

It's safer to maintain multiple generations of backups, such as daily, weekly, etc. Make sure that the backup drive is not directly accessible from the network. This can prevent the backup data from being encrypted.

・Summary

1) There is not a perfect way to completely prevent ransomware attacks. The only way is to accumulate multiple general countermeasures.

2) In the event of an attack, identify onboard data and conduct a risk assessment to minimize the damage from information leakage. Avoid placing high-risk data in shared folders. Instead, use password-protected ZIP files.

3) Backups are vital to minimize the damage to integrity and availability. Take this opportunity to verify the backup systems on each vessel and ensure they are functioning effectively. *

* ORCA's standard system includes two-generation (daily and weekly) backups stored on a separate drive from NAS.

If you have any questions, please feel free to contact us.
Thank you for your continuing support to our N-OASYS service.

Author: S.Y.Chang / ORCA
Date: 2024/7/31