KAIRIKI GROUP

October 1st, 2022

KAIRIKI CO., LTD.
7F Suzuyo Nihonbashi Building. 2-1-17 Iwamoto-cho,
Chiyoda-ku, Tokyo, 101-0032 Japan
Tel: 81-3-5846-9515 Fax: 81-3-5846-9516
Mail: info@kairiki-ships.com URL: http://kairiki-ships.com/

ISO27001

KC No. 002

Dear Valued Customers & Business Partners,

Threats of Shortcut Virus

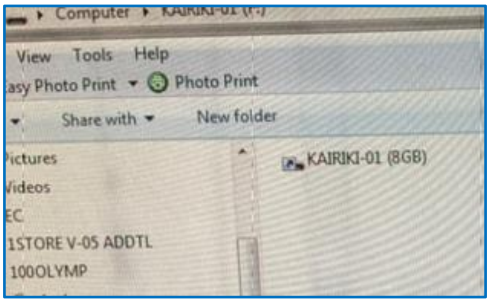
We would like to inform you of a shortcut virus that is frequently seen infecting computer aboard vessels.

What is a shortcut virus?

The shortcut virus is a malware that infects computers and creates shortcuts on the desktop, in the Windows Explorer file list, on network drives, and on USB drives. When infected, the drive or file becomes a shortcut and cannot be accessed at all, and opening the shortcut triggers the virus, which can cause serious data loss or corruption. The infection is very strong and is the most common case of virus infection on vessels

Route of infection:

- Attached file in e-mail
- URL links in the body of the e-mail
- Download from infected websites
- USB flash drive

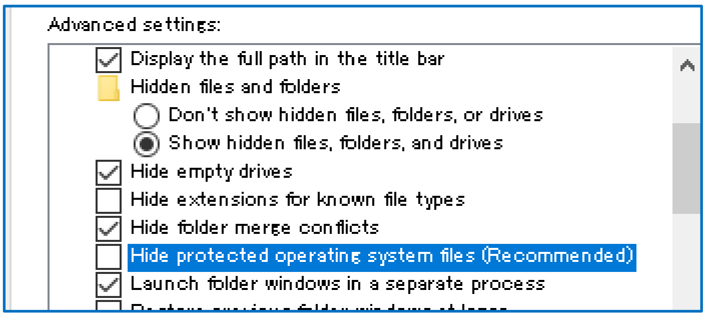


Case study

We received inquiry from a vessel that had virus infection on their computer.

When a USB flash drive was inserted into the computer, its contents became a shortcut, and eventually all computers on the vessel were infected with the shortcut virus via the infected USB flash drive.

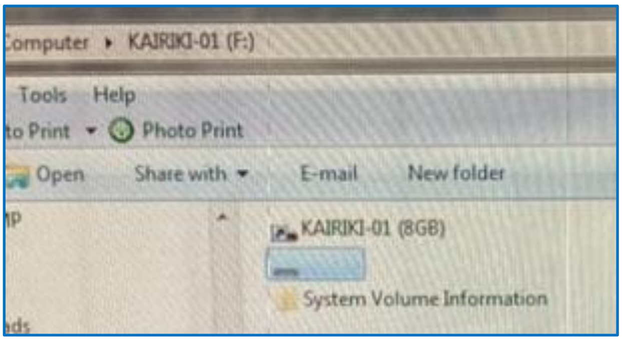
In this case, the solution was to use security software to remove the virus, rescue the hidden files, and format all infected USB flash drives.

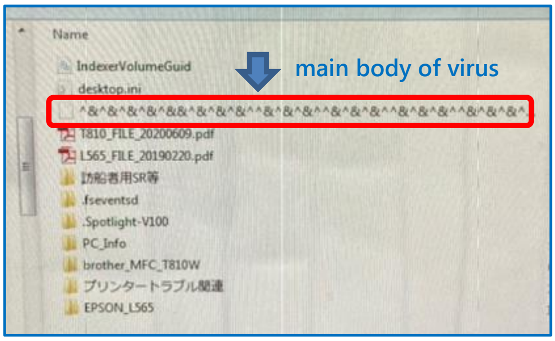


Advanced settings:

- ☑ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives
- □ Hide extensions for known file types
- ☑ Hide folder merge conflicts
- □ Hide protected operating system files (Recommended)
- ☑ Launch folder windows in a separate process

Note: When system files are set to be shown, files hidden by the virus or the virus itself may be visible.




main body of virus

By opening the hidden file instead of the shortcut in the infected USB flash drive, you might be able to find the original file.

In this case, the body of the virus exists in the hidden folder, and if the shortcut is opened, the effect the virus is triggered.

Primary action to shortcut virus infection

Never open created shortcuts! Immediately disconnect the infected computer from the network, shut it down, and report it to the responsible person.

If there are any important information in your infected computer, we recommend you talk to an expert. It might be possible to rescue your important data.

Countermeasures

a. Restrictions on who can use the computer

Only designated persons shall use computers and e-mail.

b. Managing Official USB devices

Restrict and control the usage of the USB devices provided by the company. (Prohibit to use personal USB devices)

c. Periodic updates and scans of anti-virus software

Anti-virus software is an effective way to prevent virus infection.

d. Physical blockade of USB ports

Physically seal and disable the USB port by using a special tool.

e. Data sharing without USB devices

Install NAS on LAN in the vessel to share and store data via network.

f. Installing 'visitor only' computers and printers

Provide computers and printers in a stand-alone configuration to avoid the risk of external virus intrusion.

If you have any concerns about cyber security for your vessel, we are welcome responding to your inquiries.