AccessReal

Malware&Virus Prevention and Treatment

Version 1.0

i-Sprint

Trust without Boundaries

Table of Contents

1 Precaution for Malware & Viruses

1.1 Purpose

Specify the workflow of protecting AssessReal's confidentiality, integrity and availability, and how to prevent and treat malware and viruses.

1.2 Staff Chart

IT department has to set a comprehensive workflow for malware/viruses prevention and treatment. It shall list the staffs' roles and responsibilities. Installation Virus Officer (IVO) is a team leader who is in charge of setting up the workflow to take precaution for malware and viruses, train the team members, and take action for any malware/viruses' responses.

Title	Description
IVO	Installation Virus Officer
DVA	Department Virus Administrator
NU	Normal User

Anti-malwares/viruses team members' job scopes are listed below:

1. **Installation Virus Officer (IVO)**
   - Notify the recipients when the systems are infected with malware/viruses.
   - Research on the malware/viruses that can be found on the emails or files.
   - Notify the information chief about all the malware/viruses' events and actions.
   - Reduce any lost data or information and take actions to prevent such malwares/viruses.
   - Inform the leaders to check whether to keep the precaution workflows for preventive measures, and keep updated as needed.
   - Write "Malware/Virus Respond" workflow and send it to all the system users.
   - Check the software and files used for the key business regularly after malware/virus attacks if there are any unauthorized changes.
   - Contact the vendors to obtain the anti-virus engine as needed.
   - Coordinate closely with the Department Virus Administer (DVA).
   - Manage the anti-malware/virus events for all the servers, and take actions if any malware/virus is found.
2. **Department Virus Administer (DVA)**
   - Collect all the malware/virus information such as the possible reasons and previous warning messages.
   - Locate the malware/virus infected files in the department.
   - Scan the infected files using anti-malware/virus software to check if the malware/virus still exists.
   - Determine if other files are infected by the virus, and take actions if any. Shut down

the workstation or even part of the network to avoid further infection.

- Exchange and discuss the malware/virus information with the Installation Virus Officer (IVO) and look for any other solutions.
- Update the malware/virus information to the related staffs.
- Maintain the anti-malware/virus software in the department.
- Check if the anti-malware/virus client software upgrade normally.

3. Normal User (NU)

- Follow the anti-malware/virus specifications.
- Notify DVA immediately if any malware/virus is found.
- Notify DVA immediately to check if there is any malware/virus when the machine slows down, or if there is any damaged or lost file(s).
- Check the anti-malware/virus software's version regularly. Notify DVA if the version is not updated.

1.3 Precaution Measures

i. Install the anti-malware/virus software and update the virus-based regularly for all computers that involved with AccessReal (including the virtue system, notebook, and server).

ii. IT shall check and kill malware/virus on all PCs and notebooks every month, and spot check the result.

iii. IT department shall: 1) Harden the system. 2) Monitor the security information, and notify staffs to install the system patch if any serious system bug is found. 3) Collect and feedback on the installation.

iv. Install the firewall and Intrusion Detection System, and use encryption protocol for the network that connects to an external network.

v. Do not allow a Normal User (NU) to use disk driver, U disk, or portable hard disk and others. During special conditions, those devices can be connected to the company computer device after check.

vi. Check for malware/virus at the program/ data download from the website and devices. Do not install any suspect device driver. Do not run an executable program or script on the important servers.

vii. Strengthen management for network devices such as routers and firewall. Turn on the firewall belongs to the computer. Close unused ports and protocols.

viii. Prepare and update the training files. Provide training to users regularly to learn more about the anti-malware/virus workflow and actions. Do not use any suspect software. Delete any suspect emails.

2 Actions for Malwares & Virus

Virus and worm cause different impacts. The workflows for both of them are the same except the system isolation and the scheduled time.

The worm will duplicate automatically and infect hundreds of machine in a short time. Therefore, if you are unable to find out its event type, simply follow the worm's flow for further actions.

Department Virus Administrator (DVA) to take the actions below.

2.1 Virus Signs

Use appropriate software to monitor the system's hardware, software, and the real-time statuses. For any detected unusual signs, the software will send an alarm automatically to the delegated staffs. All staffs will be alerted if their computers show the following signs:

- Longer time is taken for the computer to react or to run the apps.
- Unusual error messages are displayed.
- An unexpected flashing light is shown on the hard disk.
- The sudden reduction of system available memory.
- The sudden reduction of hard disk space and suspect process is found.
- The file size, content, extension name, date or property are being modified.
- The application access multiple hard disks concurrently.

Normal user (NU) should notify the IVO and DVA immediately, and should not open the infected files.

2.2 Action Guide

i. NU should not open the malware or virus infected files. They shall be handled by the IT staffs ASAP.

ii. Do not expose the malware or virus information to an unknown staff to avoid unexpected results. The later chapter will talk about the release message guide.

iii. Alarm configurations for malware or viruses
   - The monitoring software informs the admin console if any malware or viruses are detected. DVA shall take action when he/she receives such alarm.
   - The DVA shall inform the user to upgrade the virus database and anti-virus engine if any virus is found at the file server or the gateway server, and then scan and remove the virus for the computers.

2.3 Measure & Flow

2.3.1. Keep Logs

Logs consist of the followings.

i. Malware/virus event date and time.
ii. Flow/actions.
iii. The time that flows/actions take.
iv. Malware/virus event's effects and its results.

2.3.2. Isolate System

Isolate the malware/virus infected system with other systems of the internal network. For suspect worm event, the internal network shall be disconnected with Internet.

Disconnection of networks is a method that can stop the worm from spreading. However, network disconnection causes inconvenience for downloading the anti-virus packages from the Internet. IT department head will decide whether to disconnect or not. He/she will appoint someone to record the actions of the anti-worm.

Do not make the system outage, and do not reboot the system since some viruses may destroy the data on the disks or delete the viruses' shreds of evidence when reboot.

2.3.3. Confirm Malwares/Virus

Locate and isolate the virus or worm files and its process. Take a system snapshot and put it to a safe place before deleting files or remove the process.

When virus or worm codes are found, move them to the isolated area or store them in tape. Delete the infected files. List all active network connections, and take a snapshot together with the technical staff.

2.3.4. Kill Malwares/Virus

Kill all suspect processes. Dump the system to tape, add a tag to the tape, and then save it. Delete all suspect virus infected files or virus files. For worm event, the Internet can be connected again after all the malware or viruses are killed and precaution measures are taken.

Update the anti-virus engine and virus database to the latest, and then use those tools to check and kill the viruses.

For a known virus, go to anti-virus vendors' website to download the desired package or tools to kill the virus.

For an unknown virus, pack the suspect files and submit to the anti-virus vendors for help.

The anti-virus vendors will check these suspect files, extract the virus samples, and develop new anti-virus engines and virus definition code database, and then fix the infected files and return them to the client.

Note: To kill all viruses, isolate the viruses for those that are not attached to other files or destroyed original files.

For isolation, create isolation server, and set isolated area in this server. Next, create folders

for each department. Inside the department folder, create a folder for each staff of this department. Move the viruses that are unable to kill to the isolated folder. Set access control for the isolated server.

2.3.5. Harden System

Evaluate the system damage level, and analysis the malware codes. Then harden the system or upgrade the anti-virus software.

It is important to install necessary safety patches to fight the virus.

2.3.6. Restoration

Before carrying out the system restore, all the related staffs mentioned at section 1 shall be notified.

When the systems are working properly, all NUs shall be notified to modify their passwords.

Make sure all systems are working properly before reconnecting to the Internet. Record all actions.

2.3.7. Release Message

For serious malware/virus events, do not expose the message to undesired staffs. All messages' releases shall be approved by the company leaders or the one who is authorized by the company.

The company shall provide resources for fighting against malware/virus, and support the IT policies that can reduce risk and costs.

2.3.8. Report & Analysis

A report shall be generated after all the systems are back to normal. Gather all related staffs to discuss the events, review and modify the flows if needed. Delete all the infected files of the systems.

A report shall be taken by a specified staff, and its content can include the suggestions.

2.3.9. Virus Event Record

See next page.

Malware/virus Emergency Event List

No： _____ Date：_____ (Date/Month/Year)

Review：_____

	Founder	**Time**	**Description**		**Remarks**
Report					
	Reporter	**Time**	**Report to**	**Respond Description**	**Remarks**
Respond					
	Operator	**Time**	**Guide**	**Actions Description**	**Remarks**
Actions					
	Operator	**Time**	**Emergency Respond Description**		**Remarks**
Emergency Respond					

Malware/virus Event Overview	