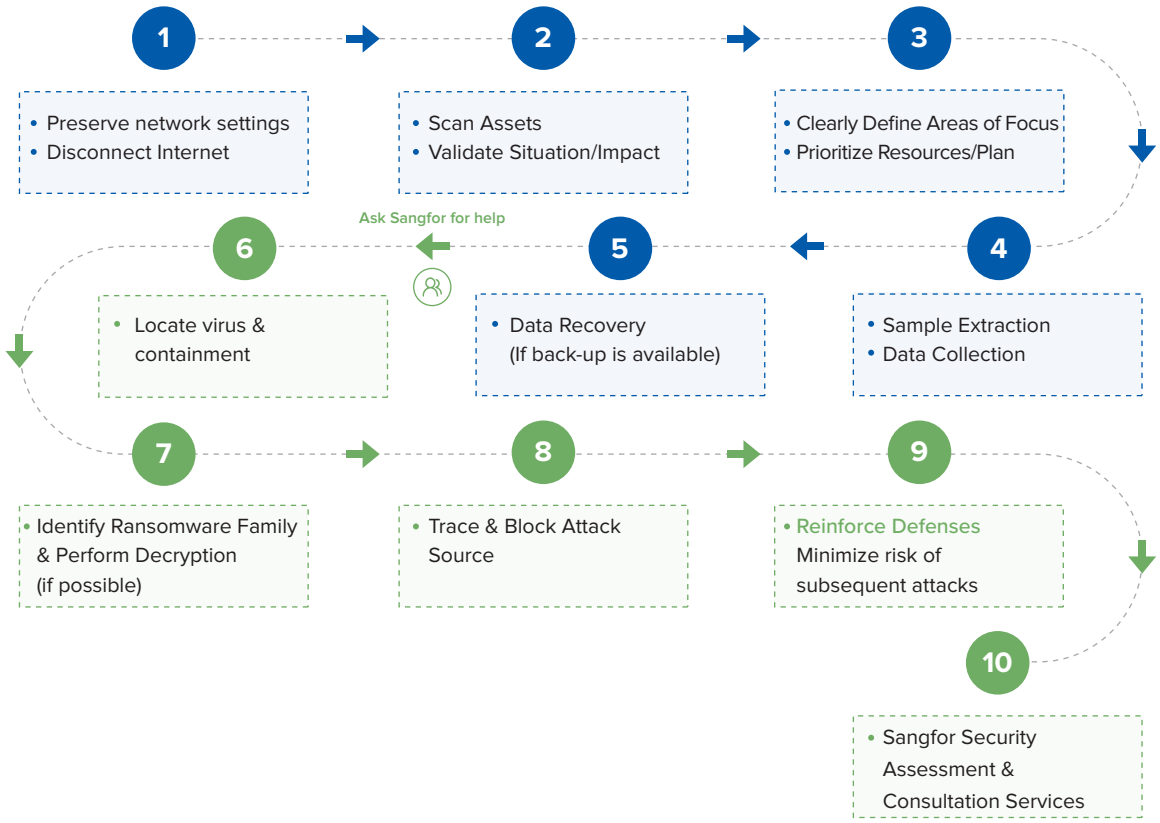
# Ransomware Response Playbook

## Sangfor Incident Response Services

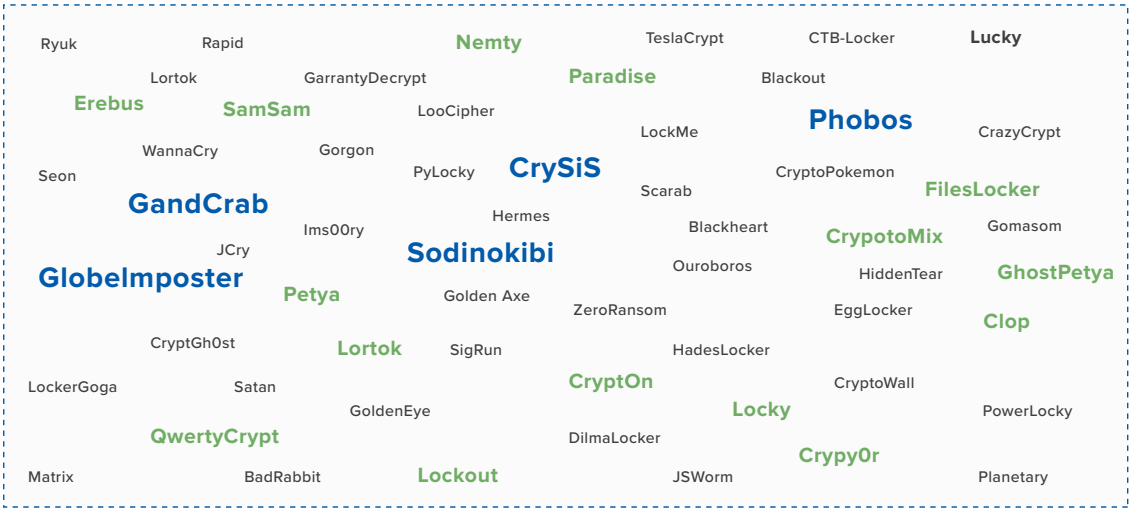
www.sangfor.com

SANGFOR

## Action Guidelines




Have you been attacked by ransomware? Ransomware attacks can cause network failure, data encryption and business interruption. How do you determine if your data can be decrypted and recovered? How do you reinforce your defenses and regain stability? Sangfor has the answer in these 10 easy steps.




Sangfor has an in-depth knowledge of ransomware analysis and professional incident response services, having tracked over 200 ransomware families and over 1000 variants. In the event of a ransomware attack, contact Sangfor immediately for free ransomware consultation and support.

## 1. Preserve Network Settings & Disconnect Internet

In the event of a disaster, any hosts who have come under attack should be isolated from the network immediately. Sangfor recommends physical isolation such as disconnecting the network cable to prevent further spread and secondary damage.

It's not imperative that unaffected hosts be disconnected, but best practice dictates that hosts that have not yet been hacked should also be isolated from the network until the ransomware is contained, and only then reconnected.

After the hosts are isolated, Sangfor recommends preserving all network settings, environment and format for any traceability forensics and analysis of the cause of the intrusion. Not preserving the settings will make it difficult for subsequent defense reinforcement, decryption and recovery. Do not power off or restart the host. If you can't wait for data recovery, employ a professional to start the process to avoid causing further damage to your network and system.

## 2. Scan Assets, Validate Situation / Impact

When attacked by ransomware, first scan your assets and confirm the validity of the attack situation. Gather the assets listed in the table below, and determine if they have been hacked. Determine which systems (servers, PCs, etc.) have been hacked and what type of ransomware has been used for the attack.

This is a sample.

| Assets IP | Use | Department | Manager | Situation |
|---|---|---|---|---|
| 192.168.0.1 | Domain Controller Server | IT Department | xx | All files are encrypted into suffixes .Pig666 |
| 192.168.0.2 | Database Server | Database Center | xx | All files are encrypted into suffixes .Krab |
| 172.168.1.102 | Personal PC | R&D | xx | All files are encrypted into suffixes .Pig666 |
| 172.168.2.103 | Personal PC | Marketing | xx | All files are encrypted into suffixes .ryk |

## 3. Clearly Define Areas of Focus, Prioritize Resources / Plan

Immediately determining the order of importance for affected systems allows emergency responders to work in on the most urgent tasks first. Focus on determining what tasks are most critical (data decryption, reinforcement defense, intrusion analysis, trace source forensics, sample analysis, enterprise intranet security status assessment, etc.).

## 4. Sample Extraction, Data Collection

Extract the system log: Copy the C:\Windows\System32\winevt directory to the desktop, and then compress it on the desktop into a compressed package named after the host, for example: 192.168.1.1-windows-log.zip

Extracting Encrypted Files: Select a number of smaller encrypted files for later decryption tests and for determining the ransomware family.

### 4.1 Determine if the ransomware is still encrypting

Use the "everything" file search tool to search for encrypted files, for example, file encryption suffix "Ares666," then search for "*.Ares666," sort by modification time, and determine if the file is encrypted.

If it is determined to be encrypted, shutdown immediately and preserve the condition of the disk for later analysis. If this step has stopped the encryption process, proceed to the following steps.

### 4.2 Determine if the ransomware is still within the hosts

Since ransomware usually encrypts any shared folders it has access to, the virus files may not be within an encrypted host.

Determine how many of the folders are encrypted. Generally, ransomware encrypts a majority of a disk, leaving several system folders (i.e. Windows) untouched, to ensure normal operation of the system. If only some folders are determined to be encrypted, you can assume the situation will be the same for shared folders. Determine if the encrypted folder properties are shared to determine if the ransomware is still within the hosts.

### 4.3 Collect system log files

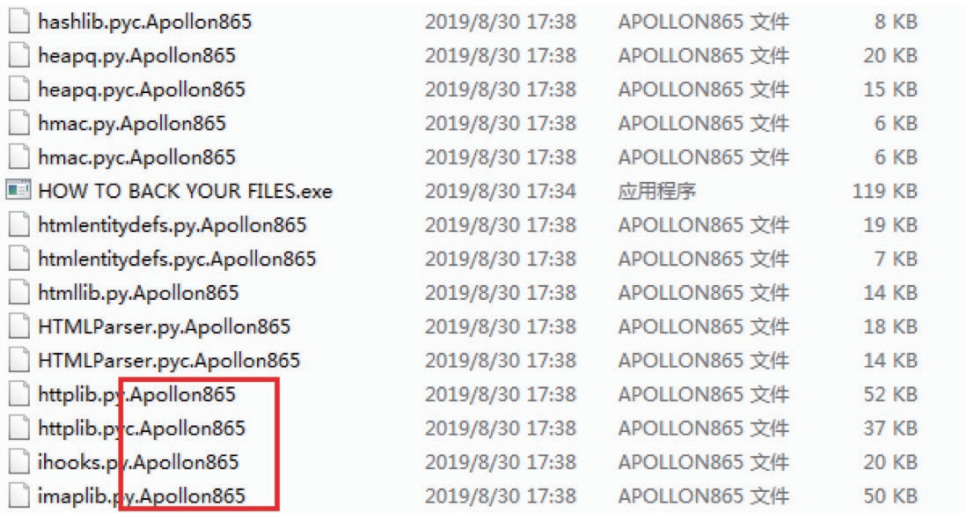
Access "C:\Windows\System32\winevt\Logs" to view the system log. The file will be very large before compression. Direct compression will often fail, as the file is occupied. Copy the logs directory to the desktop and compress.

### 4.4 Collect Ransomware Family Information

The encrypted file is not a sample. You must save the complete encrypted suffix and ransom text/pop-up window or screenshot. Please note that the screenshot must be complete and clear.

Sample ransomware of encryption screenshot:


Encrypted file suffix:



### 4.5 Search Ransomware Files

Ransomware files are usually newer and can be searched using the "everything" file search tool searching "*.exe". Sort by modification time (or creation time).

If attempting to determine possible virus-infected files by directory and file name, the most likely directories are:

"C:\Windows\Temp"
"C:\Users\[user]\AppData\Local\Temp"
"C:\Users\[user]\Desktop"
"C:\Users\[user]\Downloads"
"C:\Users\[user]\Pictures", etc.

The virus file name will masquerade as a system file, such as "svchost.exe", "WindowsUpdate.exe", or will have a clear encryption suffix, such as "Ares.exe" or "Snake.exe". Some files will have irregular names like "dll.exe". Search for irregular exe files. They may be in the name of an administrator or another specific person.

After using this method of discovering suspicious files, run VirusTotal (calculating md5 queries, preferably not directly uploading files), running them in a virtual machine, or providing them directly to the Sangfor Security Team.

In most cases, virus files can be found using this method. If they are not found, use Sangfor EDR products or tools to scan for the files. In addition, because some viruses have self-deleting characteristics, it is not always possible to find virus files, for example, the CryptOn ransomware.

**Sangfor free killing tool download link:**
*http://go.sangfor.com/anti-bot-tool-20181018*

## 5. Data Recovery (If Back-up is Available)

Sangfor after-sales engineers will come to assist customers in recovering their back-ups as quickly as possible. Customers can contact Sangfor international CTI (Malaysia) or Hong Kong support center. The telephone number & mail address are as follows:

**Sangfor International CTI (Malaysia):** 0060-0127117129 / 0060-0127117511
**Sangfor Hong Kong Support Center:** tech.support@sangfor.com.hk

## Sangfor Incident Response Services

## Customer Success Stories

### Customer A: Government

| Country | Ransomware | Response Timeline | Sangfor Solution |
|---|---|---|---|
| China | WannaCry | Recover Back-Up (1 hour)<br>Virus Type Confirmation and Infected File Isolation (30 mins)<br>ES Virus Removal (2 hours) | NGAF +<br>Endpoint Secure + SIP |

### Customer B: Education

| Country | Ransomware | Response Timeline | Sangfor Solution |
|---|---|---|---|
| Malaysia | GandGrab V2.1 | Recover Back-Up (5 mins with Sangfor HCI)<br>Virus Type Confirmation and Infected File Isolation (30 mins)<br>ES Virus Removal (2 hours) | NGAF +<br>Endpoint Secure |

### Customer C: Enterprise

| Country | Ransomware | Response Timeline | Sangfor Solution |
|---|---|---|---|
| UAE | Phobos | Virus Type Confirmation and Infected File Isolation (30 mins)<br>ES Virus Removal (2 hours)<br>Vulnerability Scanning (2 hours) | NGAF +<br>Endpoint Secure |

**For Sangfor's help after a ransomware attack, please contact us immediately:**

**Sangfor International CTI (Malaysia):** 0060-0127117129 / 0060-0127117511

tech.support@sangfor.com

**Sangfor Hong Kong Support Center:** tech.support@sangfor.com.hk