

5. Ransomware Protection



SANGFOR
深信服科技

Ransomware Protection

1. What is Ransomware?

Ransomware is a new type of computer virus. After the host is infected with a ransomware file, it will run a ransomware program on the host, traverse all local disks of specified types of files for encryption operations, and the encrypted files cannot be read. Then a ransom message is generated, requiring the victim to pay a certain value of virtual currency within a specified time to restore the data, otherwise the data will be destroyed. In terms of intuitive phenomena, the phenomenon of ransomware mainly includes the following two scenarios.

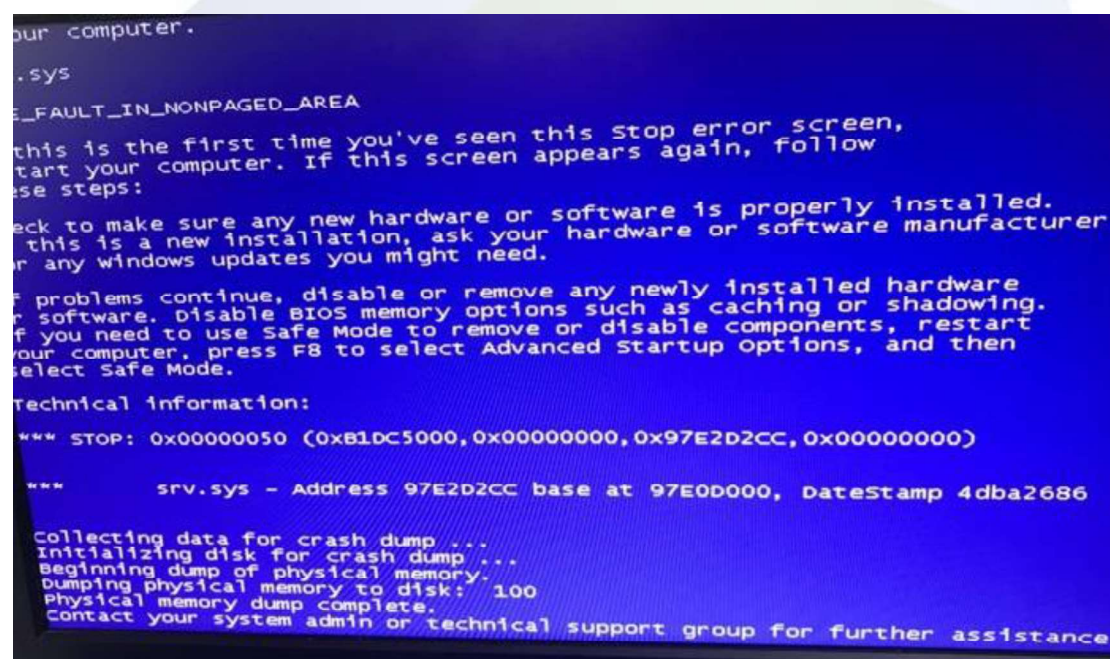
1. The server file is encrypted. For example, it is encrypted into a .java suffix or other strange suffix name, and you need to pay a certain amount of virtual currency to restore the account. If you do not pay, the data will be destroyed.



Ransomware Protection

What is Ransomware?

2. Many hosts on the intranet are experiencing blue screens. The code of the blue screen indicates that there is a problem with the **srv.sys** driver, as shown in the following figure:



Note:

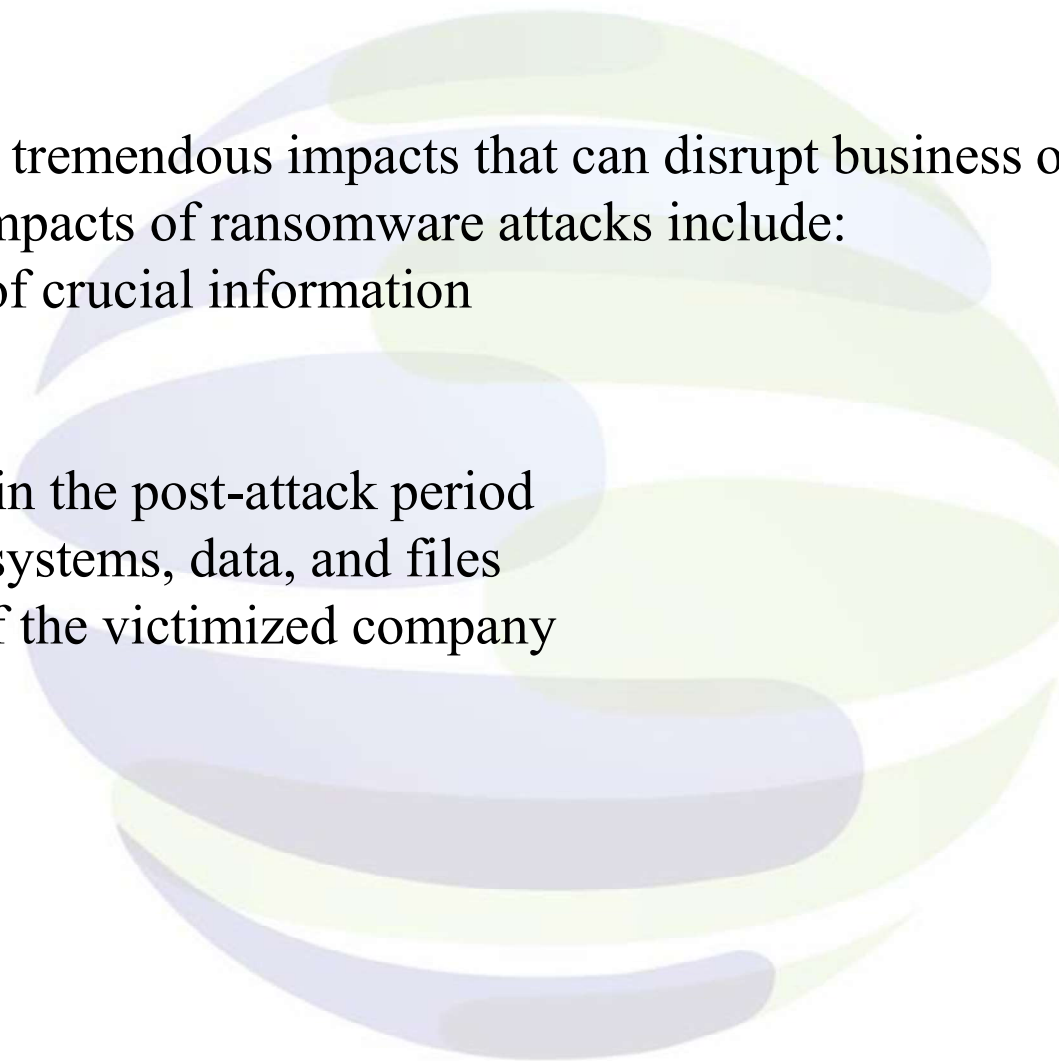
Many host blue screens on the intranet is usually a variant type of ransomware virus, which has a strong spread.

Ransomware Protection

Impacts of Ransomware

Ransomware can cause tremendous impacts that can disrupt business operations and lead to data loss. The impacts of ransomware attacks include:

- ◆ Loss or destruction of crucial information
- ◆ Business downtime
- ◆ Productivity loss
- ◆ Business disruption in the post-attack period
- ◆ Damage of hostage systems, data, and files
- ◆ Loss of reputation of the victimized company



Ransomware Protection

Protection Against Ransomware

1. **Reinforcement in advance:** Ransomware risk assessment, accurate assessment of the risk of ransomware entry points, configuration of special strategies for ransomware, and comprehensive protection of ransomware risks.
2. **Active defense in the event:** Comprehensive protection against ransomware risks through the configured special strategy for ransomware virus.
3. **Post-event quick response and disposal:** Isolate and identify the host that has been compromised and use special tools for anti-virus.

Ransomware Protection

The principle of ransomware infection

1. First, hacker will perform password brute force cracking through SMB and RDP port. It is the port that ransomware commonly used. Besides, the hacker will exploit the vulnerabilities of server and the ransomware will try to find a way to infect the host.
2. After the host is infected by ransomware, the ransom process will be executed in the host. At the same time, the hacker will manually use SMB or RDP to spread the ransomware in order to get more hosts infected.
3. When the ransomware process runs on one or more hosts, the ransomware will search through local disk and will encrypt a specific file type. Encrypted files will not be able to read.
4. It will prompt a ransom message to the victim of the computer which has been infected by ransomware. Besides, it also requires the victim to make payment by using bitcoin within a period of time in order to recover the encrypted data, or else the ransom will be double or will not decrypt the encrypted file.
5. Normally the encrypted data is not able to decrypt by itself because ransomware is using strong encryption method which makes the victim unable to decrypt the encrypted data if the victim does not have private key.

Ransomware Protection

The value of NGAF in Ransomware protection

- (1) Risk assessment of ransomware, accurately assessing the risk of entry points of ransomware.
- (2) Special protection configuration for ransomware, comprehensive protection against ransomware risks.
- (3) Special blackmail protection area, visual recognition and rapid handling of blackmail risk.

Best Practice

Vulnerability detection and realtime protection safeguard networks against ransomware attacks.



Vulnerability Detection

Detect vulnerabilities and block ransomware from infecting business assets.



Exploitation Protection

Analyze attack techniques and defend against ransomware attacks.



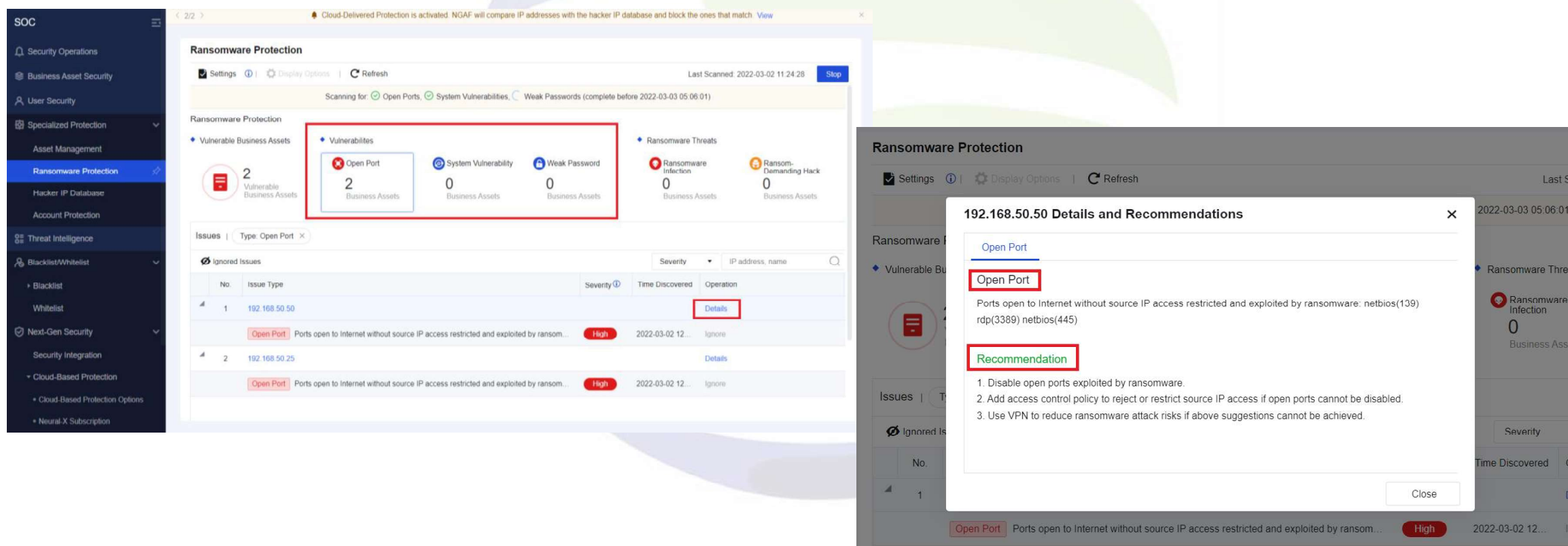
Remediation

Isolate compromised servers and remove ransomware via Endpoint Secure.

Ransomware Protection

Reinforcement In Advanced

Sort out the exposure of assets and block the entry points of ransomware. Identify common ports of ransomware, common vulnerabilities of ransomware, weak passwords in advance and give corresponding treatment suggestions.



The screenshot displays the Sangfor Ransomware Protection interface. The left sidebar shows the SOC (Security Operations Center) menu with options like Security Operations, Business Asset Security, User Security, Specialized Protection, Asset Management, Ransomware Protection (selected), Hacker IP Database, Account Protection, Threat Intelligence, Blacklist/Whitelist, Next-Gen Security, Security Integration, Cloud-Based Protection, and Neural-X Subscription.

The main panel shows the Ransomware Protection status, including a notification that Cloud-Delivered Protection is activated. It displays a summary of vulnerabilities: 2 Vulnerable Business Assets, 2 Open Port Business Assets, 0 System Vulnerability Business Assets, 0 Weak Password Business Assets, 0 Ransomware Infection Business Assets, and 0 Ransom-Demanding Hack Business Assets.

The 'Issues' section is filtered by 'Open Port'. It shows a table of issues with columns for No., Issue Type, Severity, Time Discovered, and Operation. The first issue is for IP 192.168.50.50, categorized as 'Open Port' with a 'High' severity. A 'Details' link is provided for this issue.

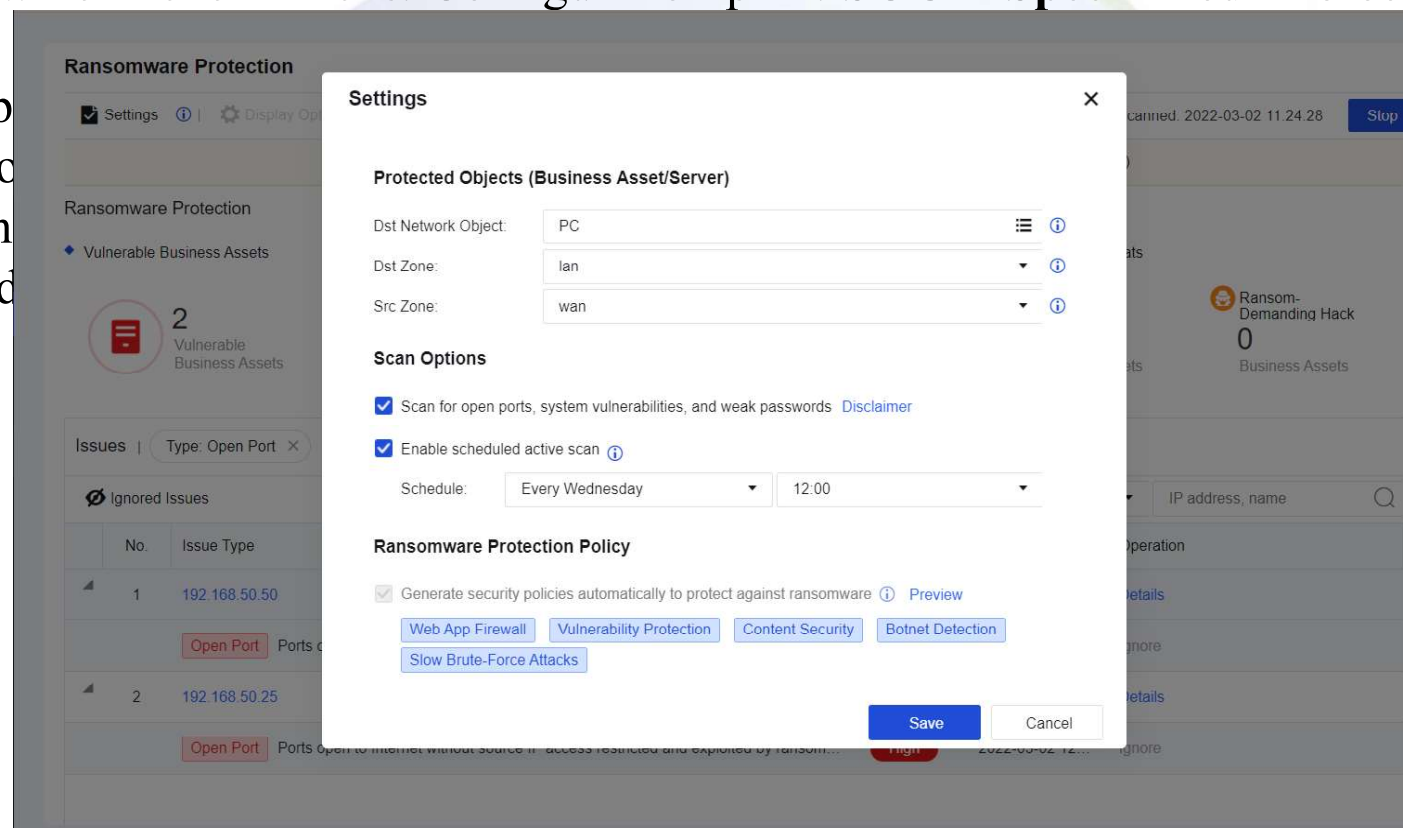
The 'Details and Recommendations' window for IP 192.168.50.50 is open, showing the 'Open Port' section. It lists the ports open to the Internet without source IP access restricted and exploited by ransomware: netbios(139) and rdp(3389) netbios(445). The 'Recommendation' section provides three suggestions:

1. Disable open ports exploited by ransomware.
2. Add access control policy to reject or restrict source IP access if open ports cannot be disabled.
3. Use VPN to reduce ransomware attack risks if above suggestions cannot be achieved.

Ransomware Protection

Defense In Event

1. The special protection policy for ransomware is automatically generated to comprehensively protect against ransomware hacker attacks. Configuration path: **SOC > Specialized Protection > Ransomware Protection.**
2. Through in-dep attacks, and co protection, vuln further analyzed



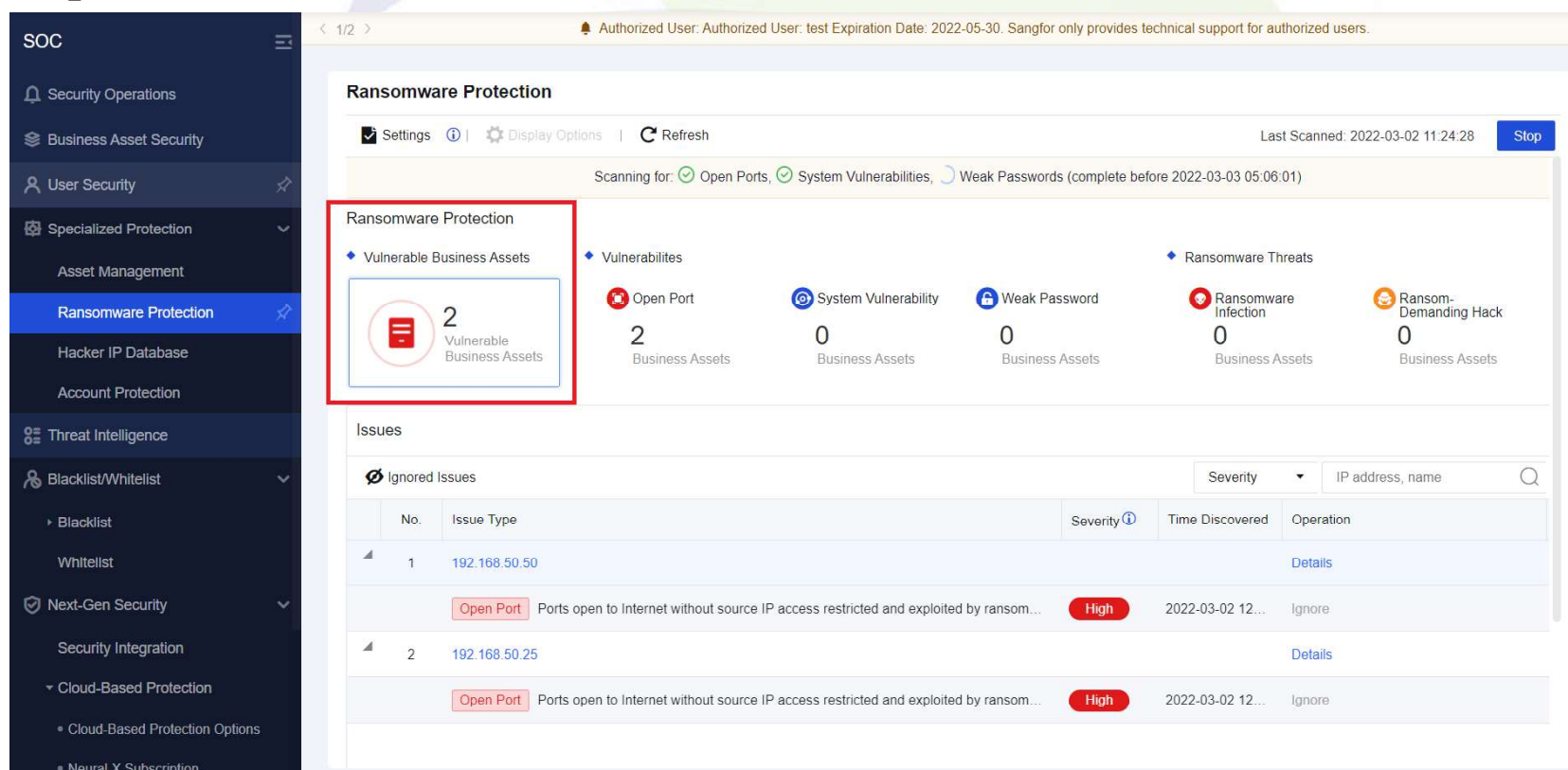
covert ransomware
gh web application
ransomware can be
S

Ransomware Protection

Post-event Response and Disposal

1. Correlate with ES to detect and scan, quarantine lost assets and quickly dispose of ransomware.
2. Further analysis of the ransom based on the ransom analysis log.

Path: **SOC > Specialized Protection > Ransomware Protection**



The screenshot displays the Sangfor SOC Ransomware Protection dashboard. The left sidebar shows the navigation menu with 'Ransomware Protection' highlighted. The main content area shows a summary of vulnerabilities and threats, with a red box highlighting the 'Vulnerable Business Assets' section. Below this, a table lists specific issues, including open ports and system vulnerabilities, with details on severity and discovery time.

Ransomware Protection

Settings | Display Options | Refresh | Last Scanned: 2022-03-02 11:24:28 | Stop

Scanning for: Open Ports, System Vulnerabilities, Weak Passwords (complete before 2022-03-03 05:06:01)

Ransomware Protection Summary:

- Vulnerable Business Assets: 2
- Vulnerabilities: 2 Open Port, 0 System Vulnerability, 0 Weak Password
- Ransomware Threats: 0 Ransomware Infection, 0 Ransom-Demanding Hack

Issues

Ignored Issues

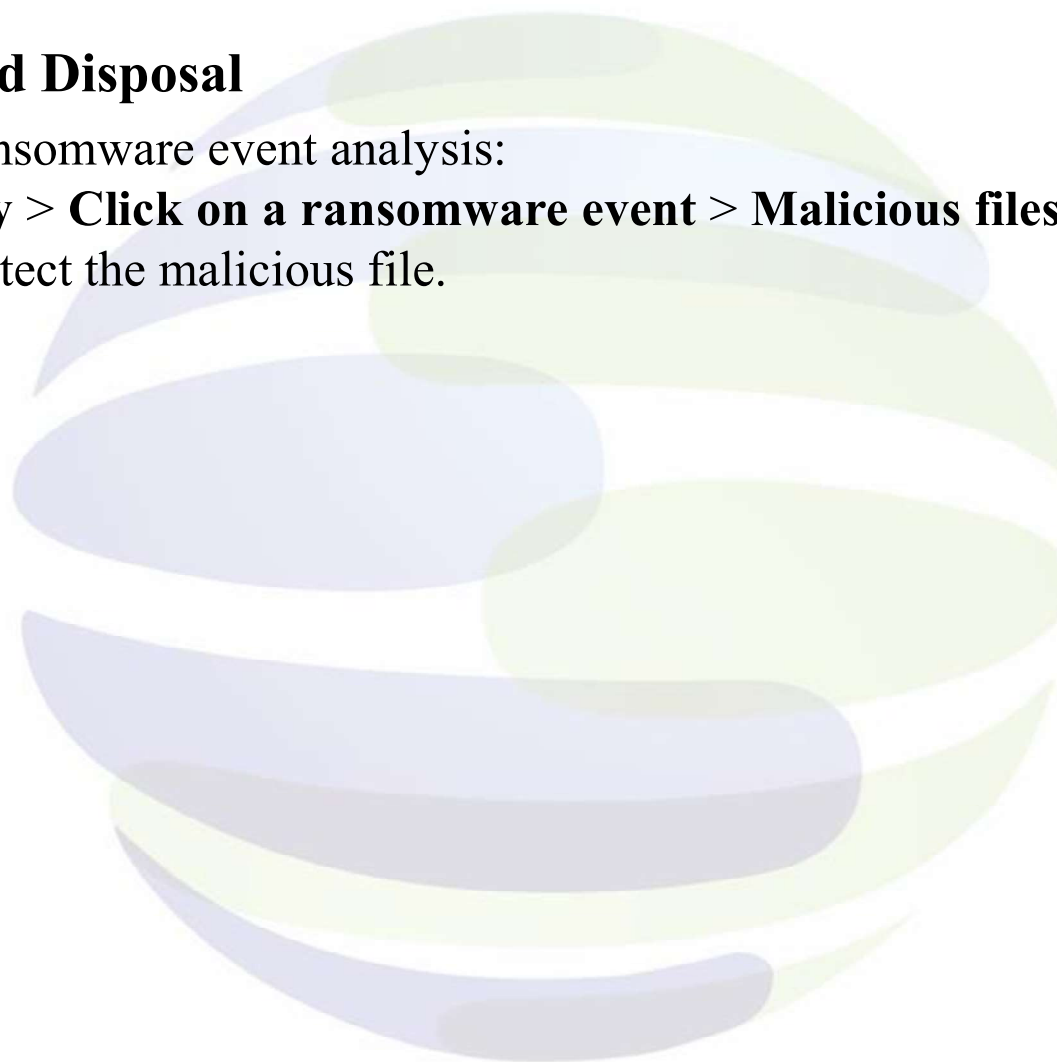
No.	Issue Type	Severity	Time Discovered	Operation
1	192.168.50.50	High	2022-03-02 12...	Details
2	192.168.50.25	High	2022-03-02 12...	Details

Ransomware Protection

Post-event Response and Disposal

3. Ransomware analysis, ransomware event analysis:

Go to **SOC > User Security > Click on a ransomware event > Malicious files**. It need to correlate the NGAF with CC only can detect the malicious file.



Ransomware Protection

5. Ransomware Protection Guide

- (1) Block or close unnecessary SMB(139,445) and RDP(3389) port.
- (2) Go to **SOC > Specialized Protection > Ransomware Protection** configure Related security policy.
- (3) The best ransomware protection method is NGAF + Endpoint.

Note: The Ransomware Protect maximum support 1024 IP for the protection.

