SANGFOR

Endpoint Secure

Best Practices for Scenarios_Prevent Brute Force Attack to Anti Ransomware

Version 3.2.22

Change Log

Date	Change Description
Feb 25, 2021	Document release.
May 17, 2021	Document update.

CONTENT

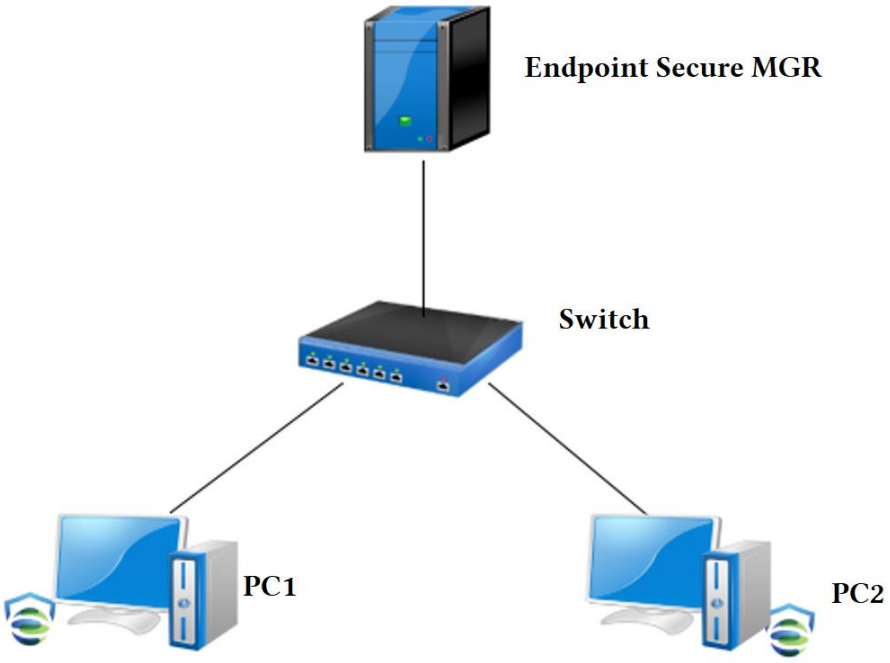
Chapter 1 Overview

This program demonstrates the process and effect of ransomware attacks when the endpoint does not run the Endpoint Secure Agent, as well as the detection and protection effect against ransomware attacks after deploying the Endpoint Secure Agent. It is suitable for showing customers how the Endpoint Secure Agent detects ransomware attacks and provides protection.

Chapter 2 Preparation for Demonstration

2.1 Environment

2.1.1 Network Environment



Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.3	PC initiating ransomware attacks
PC2	administrator/111111	20.10.0.8	PC attacked by ransomware with RDP brute-force cracking
MGR	admin/Endpoint secure@support	20.10.0.100	Endpoint Secure MGR

2.2 Attacking Process

The virus sample is put in C:/windows/evil of PC 1. During the attack, the virus first cracks PC 2 on the same LAN via RDP brute-force attack. After the cracking is completed, computer files on the local PC (PC 1), as well as computer files on PC 2, are encrypted.

2.3 Content

Stage	Content	Expected Result
Brute Force Attack	Demonstrate the attacking process and effect of ransomware without enabling the protection policy for PC 1 and PC 2 on the Endpoint Secure Agent.	1. Files on PC 1 are encrypted by ransomware. 2. PC 2 is cracked. Ransomware spreads to the LAN through RDP, and PC 2 files are encrypted.

2.4 Description

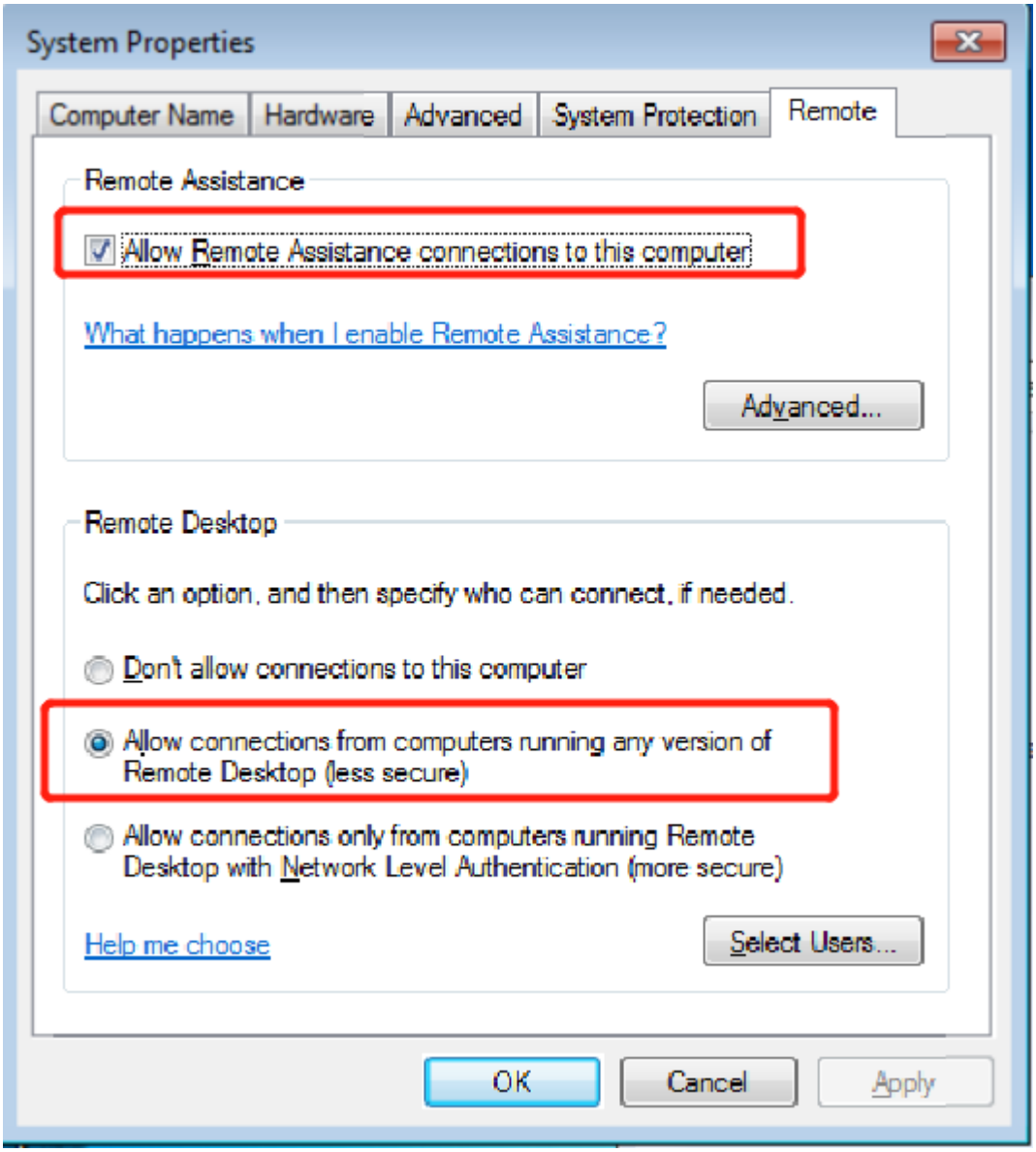
(1) This demonstration is only applicable to the virtualization environment deployed on a client or personal computer, and the demonstration environment needs to be isolated from the customer business network, so as to prevent ransomware from encrypting other computers.

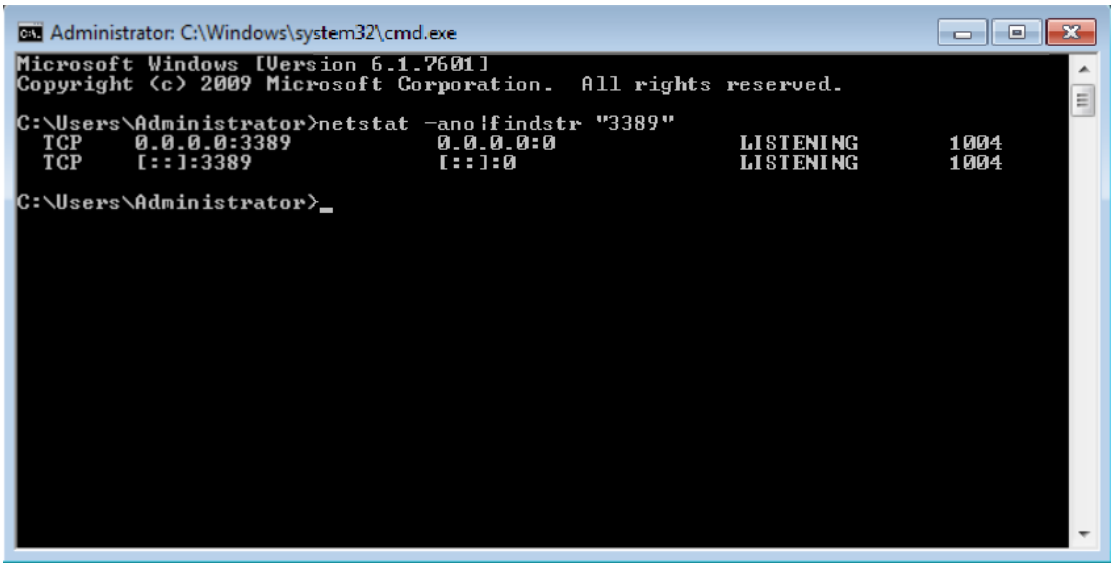
(2) You can set up MGR, PC 1, and PC 2 by yourselves. PC 1 and PC 2 need to install the Endpoint Secure Agent.

(3) Usually, PC 1 and PC 2 run Windows 7 SP1.

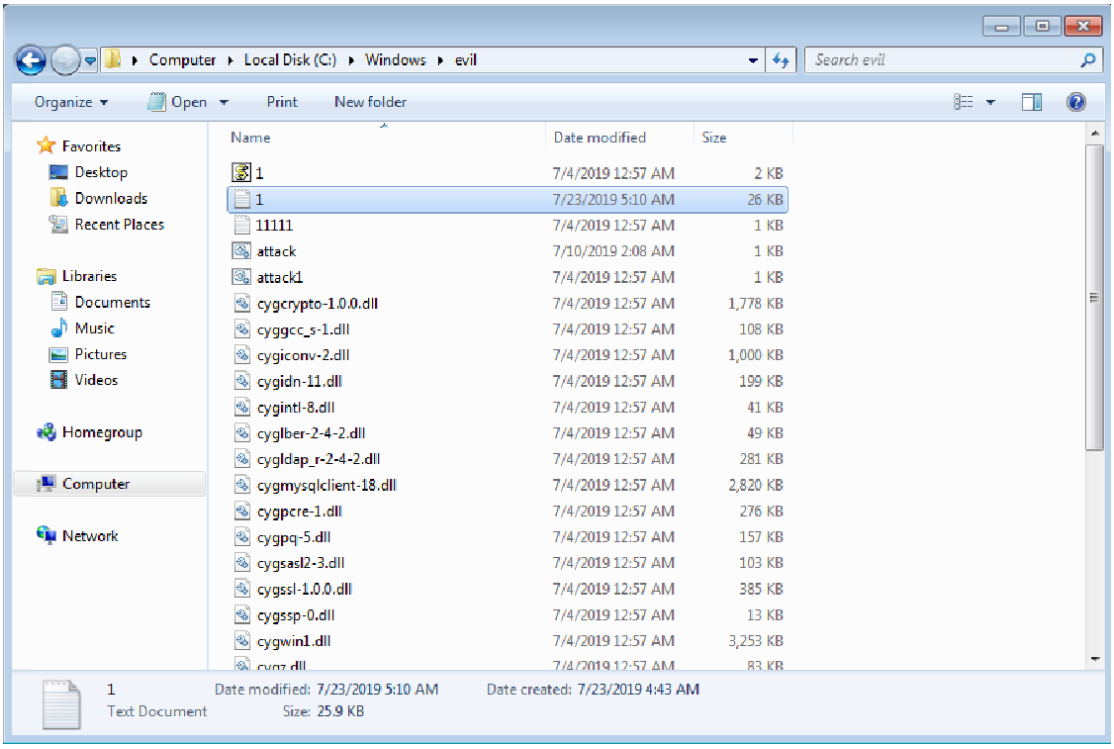
(4) PC 1 and PC 2 can use the addresses of network segment 20.10.0.0/24. The ransomware program will automatically scan other PCs on the same network segment.

(5) You are advised to turn off the system firewall of Windows and enable the RDP service of PC 2 as ransomware will crack through port 3389 of PC 2.

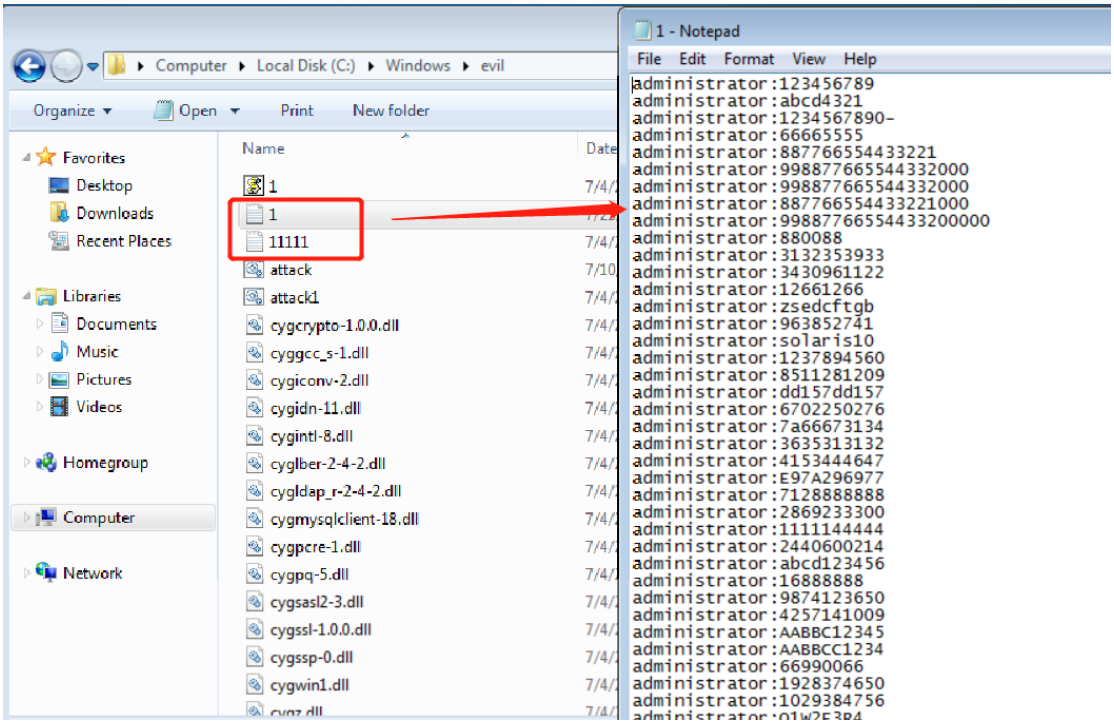




(6) The ransomware sample needs to be put in a specific directory.



(7) Passwords used for virus cracking cover those normally recorded in text files. Therefore, when using your own Windows 7 system, make sure that the passwords used are covered by the text file (containing normal passwords) in the virus toolkit. It is recommended to use administrator/111111 as the username and password.



2.5 Risks

Risk Item	Description
Isolation of demonstration	Since ransomware is run, the demonstration will be

environment	carried out in a virtual environment and needs to be isolated from the real network. If failing to do so, other computer files on the network will be attacked by ransomware.
Snapshot of the PCs used for demonstration	During the demonstration, PC files will be encrypted by ransomware. To quickly restore to the previous status for the next round demonstration, you need to snapshoot the PC in advance.

Chapter 3 Demonstration Process

3.1 Round

3.1.1 Content

On the Endpoint Secure Agent, enable the protection policy for PC 1 and PC 2 (for detection and blocking of brute-force attack), and demonstrate the attacking process and effect of ransomware.

3.1.2 Expected Results

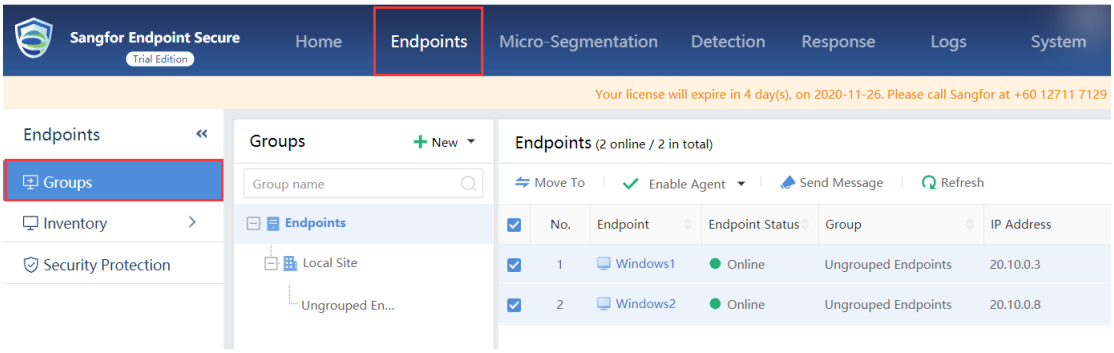
PC 1 and PC 2 are protected by the Endpoint Secure policy against brute-force attacks, which blocks virus cracking and spread. As a result, files are not encrypted by ransomware.

3.1.3 Steps

3.1.3.1 Restoring from Snapshots

(1) Roll back PC 1 and PC 2 to the previous status using their snapshots.

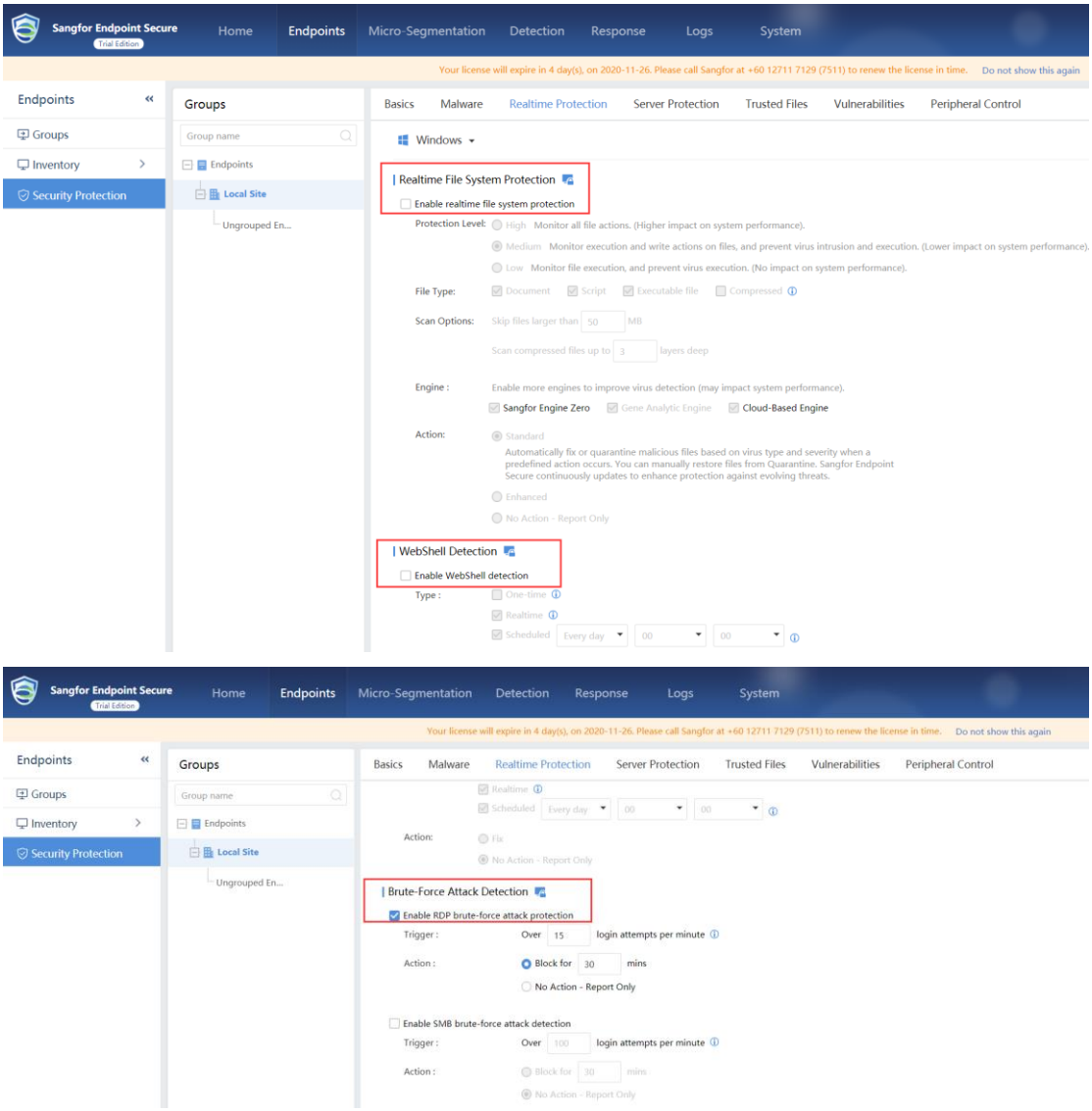
(2) Check MGR and find that both PC 1 and PC 2 get online, as shown below:



3.1.3.2 Policy Setting

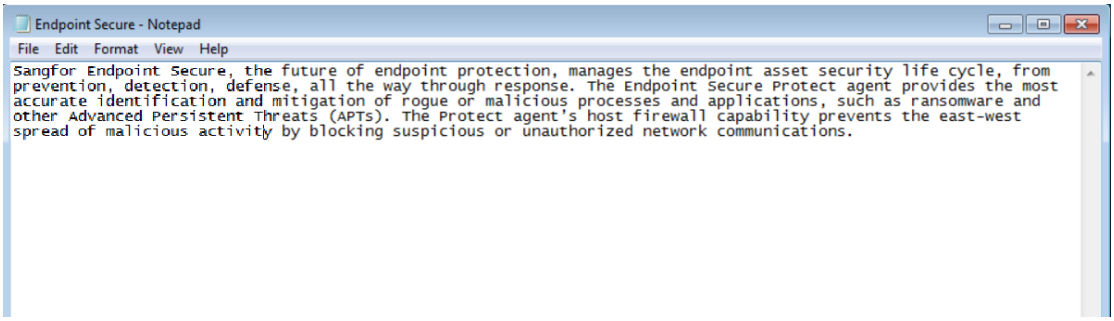
Set the security policy. Enable the policy of detecting and blocking brute-force attacks, and disable other real-time protection policies.

Choose **Endpoints** > **Security Protection**. Set the **Ungrouped Endpoints** policy (both PC 1 and PC 2 get online on ungrouped endpoints by default) and go to the **Realtime Protection** tab. Disable other real-time protection policies, such as **Realtime File System Protection**, **Ransomware Protection**, and **Advanced Threat Protection**. Turn on the lock icon. Enable **RDP brute-force attack protection** and check **Block for XX mins**, as shown below:

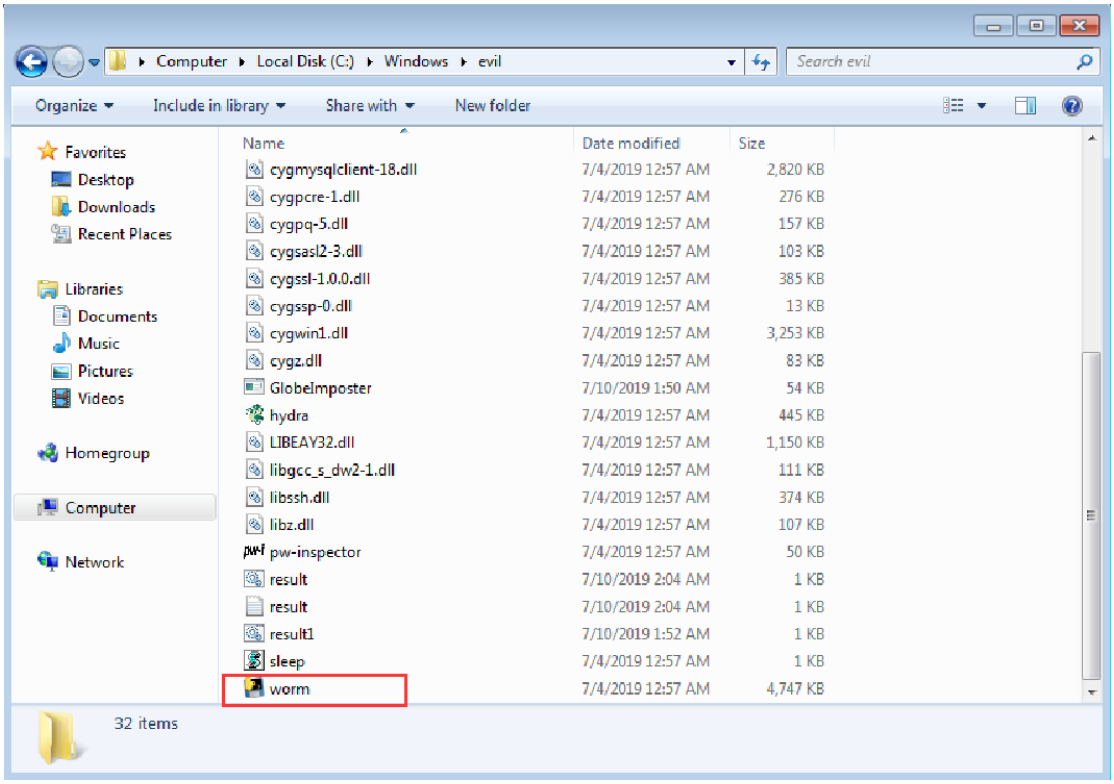


3.1.3.3 Initiating an Attack

(1) Before initiating an attack, check the status of PC 1 and PC 2. Their computer files are not encrypted and can be normally opened, as shown below:



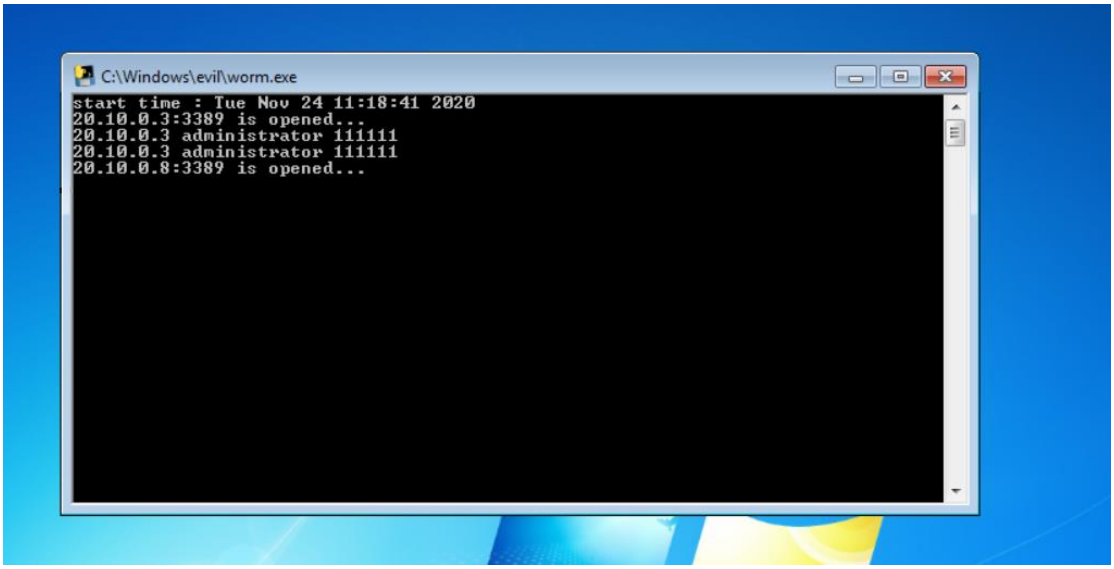
(2) Run ransomware on PC 1, as shown below:



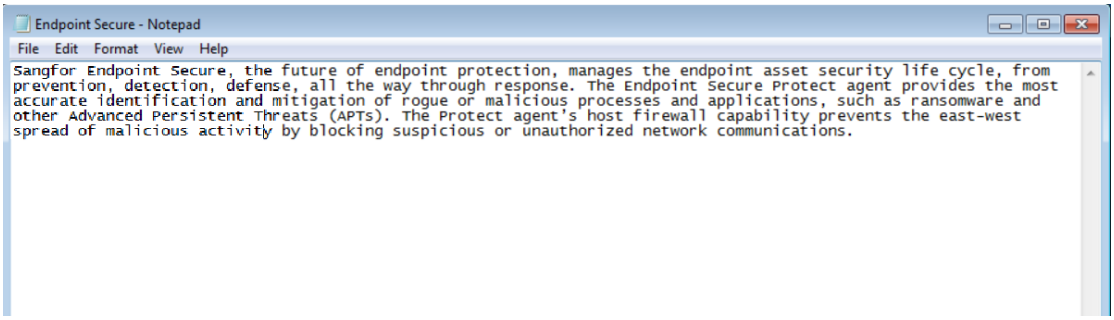
3.1.3.4 Attacking Effect

The virus attacks in such a way as cracking both PC 1 and PC 2, encrypting PC 1 files, and spreading to the LAN and encrypting PC 2 files. In this round, the Endpoint Secure Agent runs the policy against brute-force attacks to block cracking. Therefore, virus cracking fails, and files on PC 1 and PC 2 are not encrypted. You can see the cracking blocking logs on the Endpoint Secure Agent.

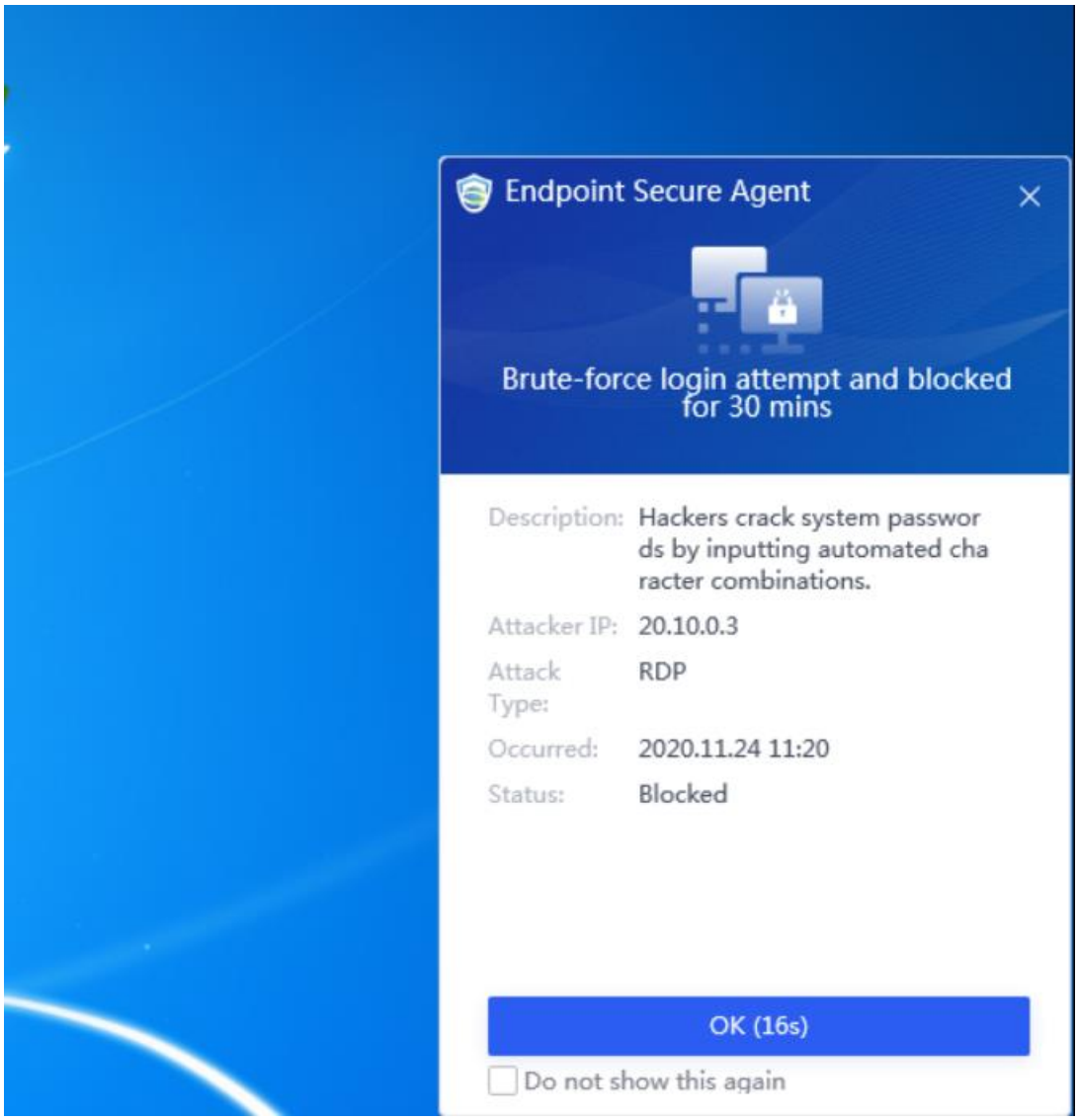
Log in to PC 1. You can find that the virus attack stops, as shown below (since Endpoint Secure blocks cracking on PC 2, the virus cannot spread further).

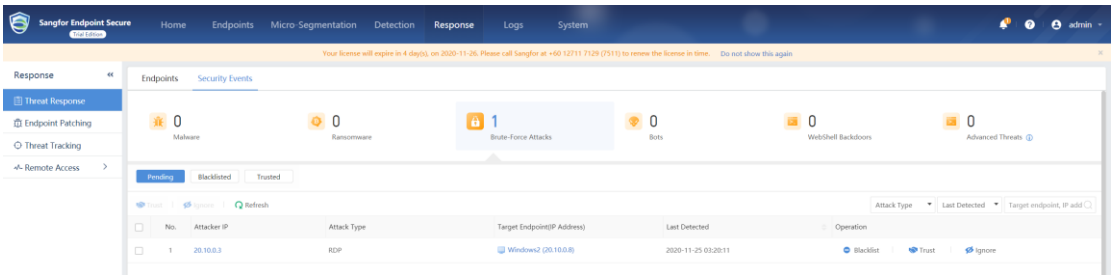


Check and find that computer files on both PC 1 and PC 2 are not encrypted. See the figure below:



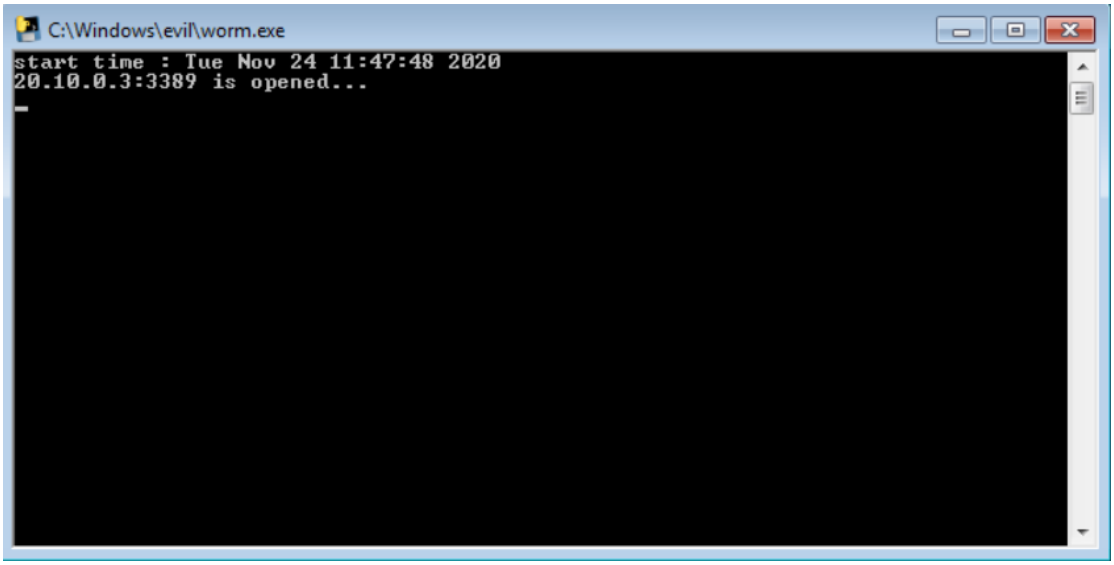
View the logs of brute-force attacks on the Endpoint Secure Agent. Choose **Response** > **Threat Response** -> **Security Events** > **Brute-Force Attacks**. The brute-force attack initiated from PC 1 has been successfully blocked, as shown below:





Chapter 4 Precautions

1. When the virus program runs, the system may stop responding sometimes and is stuck at the following position for 2 minutes. In this case, you should close and restart the program.



2. brute force attack threshold

RDP brute force attack threshold:

Quick detection mode: Configure in web console

Slow detection mode: 100 login failures within 20 minutes

Distributed detection: the same user fails to log in on 8 IP addresses within 60 seconds

SMB brute force attack threshold:

Quick detection mode: Configure in web console

Slow detection mode: 200 login failures within 20 minutes

Distributed detection: the same user fails to log in on 16 IP addresses within 60 seconds