SANGFOR

Endpoint Secure Best Practices untuk Skenario Mencegah Serangan Brute Force ke Anti Ransomware

Versi 3.2.22

Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Feb 2021	Dokumen diterbitkan.
17 Mei 2021	Dokumen diperbaharui

Daftar Isi

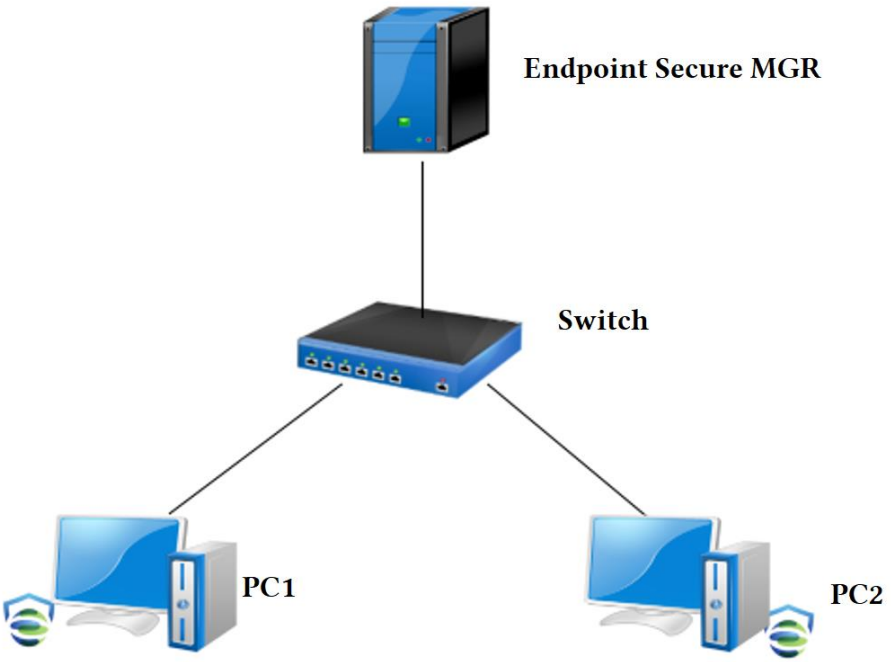
Bagian 1 Gambaran

Program ini mendemonstrasikan proses dan efek saat ransomware menyerang endpoint yang tidak menjalankan agen Endpoint Secure, selain itu efek pendeteksi dan perlindungan setelah memasang agen Endpoint Secure. Hal itu sangat cocok untuk menunjukkan kepada pelanggan bagaimana agen Endoint Secure mendeteksi serangan ransomware dan menyediakan perlingdungan.

Bagian 2 Persiapan untuk Demonstrasi

2.1 Kondisi

2.1.1 Kondisi Network

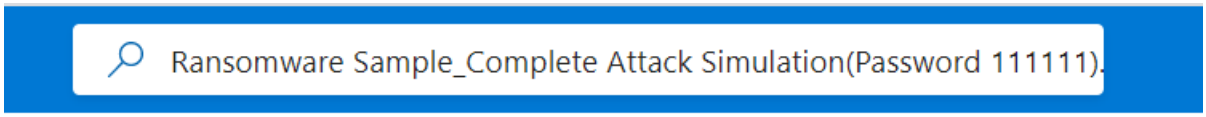


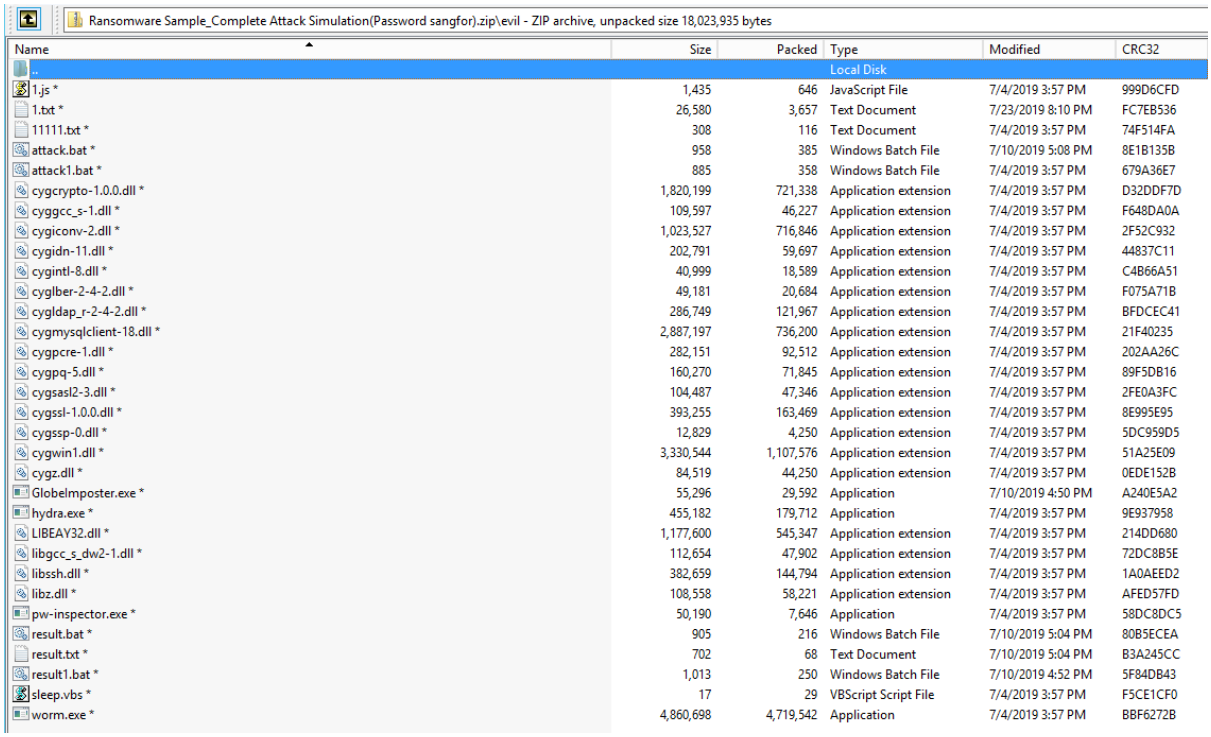
Perangkat	Account/Password	IP	Deskripsi
PC1	administrator/111111	20.10.0.3	PC yang menginisiasi serangan ransomware
PC2	administrator/111111	20.10.0.8	PC yang diserang ransomware dengan RDP brute-force cracking

MGR	admin/Endpoint secure@support	20.10.0.100	Endpoint Secure MGR

2.1.2 Contoh Virus

Untuk menyimulasikan keseluruhan proses penyerangan, anda dapat mengunduh **Ransomware Sample_Complete Attack Simulation(Password 111111).zip** di PMO.





Name	Size	Packed	Type	Modified	CRC32
..			Local Disk		
1.js *	1,435	646	JavaScript File	7/4/2019 3:57 PM	999D6CFD
1.txt *	26,580	3,657	Text Document	7/23/2019 8:10 PM	FC7EB536
11111.txt *	308	116	Text Document	7/4/2019 3:57 PM	74F514FA
attack.bat *	958	385	Windows Batch File	7/10/2019 5:08 PM	8E1B135B
attack1.bat *	885	358	Windows Batch File	7/4/2019 3:57 PM	679A36E7
cygcrypto-1.0.0.dll *	1,820,199	721,338	Application extension	7/4/2019 3:57 PM	D32DDF7D
cyggcc_s-1.dll *	109,597	46,227	Application extension	7/4/2019 3:57 PM	F648DA0A
cygiconv-2.dll *	1,023,527	716,846	Application extension	7/4/2019 3:57 PM	2F52C932
cygidn-11.dll *	202,791	59,697	Application extension	7/4/2019 3:57 PM	44837C11
cygintl-8.dll *	40,999	18,589	Application extension	7/4/2019 3:57 PM	C4B66A51
cyglber-2-4-2.dll *	49,181	20,684	Application extension	7/4/2019 3:57 PM	F075A71B
cygldap_r-2-4-2.dll *	286,749	121,967	Application extension	7/4/2019 3:57 PM	BFDCEC41
cygmysqlclient-18.dll *	2,887,197	736,200	Application extension	7/4/2019 3:57 PM	21F40235
cygpcre-1.dll *	282,151	92,512	Application extension	7/4/2019 3:57 PM	202AA26C
cygpq-5.dll *	160,270	71,845	Application extension	7/4/2019 3:57 PM	89F5DB16
cygsasl2-3.dll *	104,487	47,346	Application extension	7/4/2019 3:57 PM	2FE0A3FC
cygssl-1.0.0.dll *	393,255	163,469	Application extension	7/4/2019 3:57 PM	8E995E95
cygssp-0.dll *	12,829	4,250	Application extension	7/4/2019 3:57 PM	5DC959D5
cygwin1.dll *	3,330,544	1,107,576	Application extension	7/4/2019 3:57 PM	51A25E09
cygz.dll *	84,519	44,250	Application extension	7/4/2019 3:57 PM	0EDE152B
GlobeImposter.exe *	55,296	29,592	Application	7/10/2019 4:50 PM	A240E5A2
hydra.exe *	455,182	179,712	Application	7/4/2019 3:57 PM	9E937958
LIBEAY32.dll *	1,177,600	545,347	Application extension	7/4/2019 3:57 PM	214DD680
libgcc_s_dw2-1.dll *	112,654	47,902	Application extension	7/4/2019 3:57 PM	72DC8B5E
libssh.dll *	382,659	144,794	Application extension	7/4/2019 3:57 PM	1A0AEED2
libz.dll *	108,558	58,221	Application extension	7/4/2019 3:57 PM	AFED57FD
pw-inspector.exe *	50,190	7,646	Application	7/4/2019 3:57 PM	58DC8DC5
result.bat *	905	216	Windows Batch File	7/10/2019 5:04 PM	80B5ECEA
result.txt *	702	68	Text Document	7/10/2019 5:04 PM	B3A245CC
result1.bat *	1,013	250	Windows Batch File	7/10/2019 4:52 PM	5F84DB43
sleep.vbs *	17	29	VBScript Script File	7/4/2019 3:57 PM	F5CE1CF0
worm.exe *	4,860,698	4,719,542	Application	7/4/2019 3:57 PM	BBF6272B

2.2 Proses Penyerangan

Contoh virus diletakkan di C:/windows/evil pada PC 1. Selama penyerangan, pertama virus akan menyusup PC 2 karena memiliki LAN yang sama menggunakan RDP brute-force attack. Setelah penyusupan selesai, file pada kumputer lokal (PC 1), kemudian juga file pada komputer 2, semua terenkripsi.

2.3 Isi

Tingkatan	Isi	Hasil yang diharapkan
Brute Force	Mendemonstrasikan proses penyerangan dan efek dari ransomware	1. File pada PC 1 terenkripsi oleh ransomware.

Attack	tanpa mengaktifkan protection policy untuk PC 1 dan PC 2 pada agen Endpoint Secure.	2. PC 2 telah terserang. Ransomware menyebar ke LAN melalui RDP, dan file pada PC terenkripsi.

2.4 Penjelasan

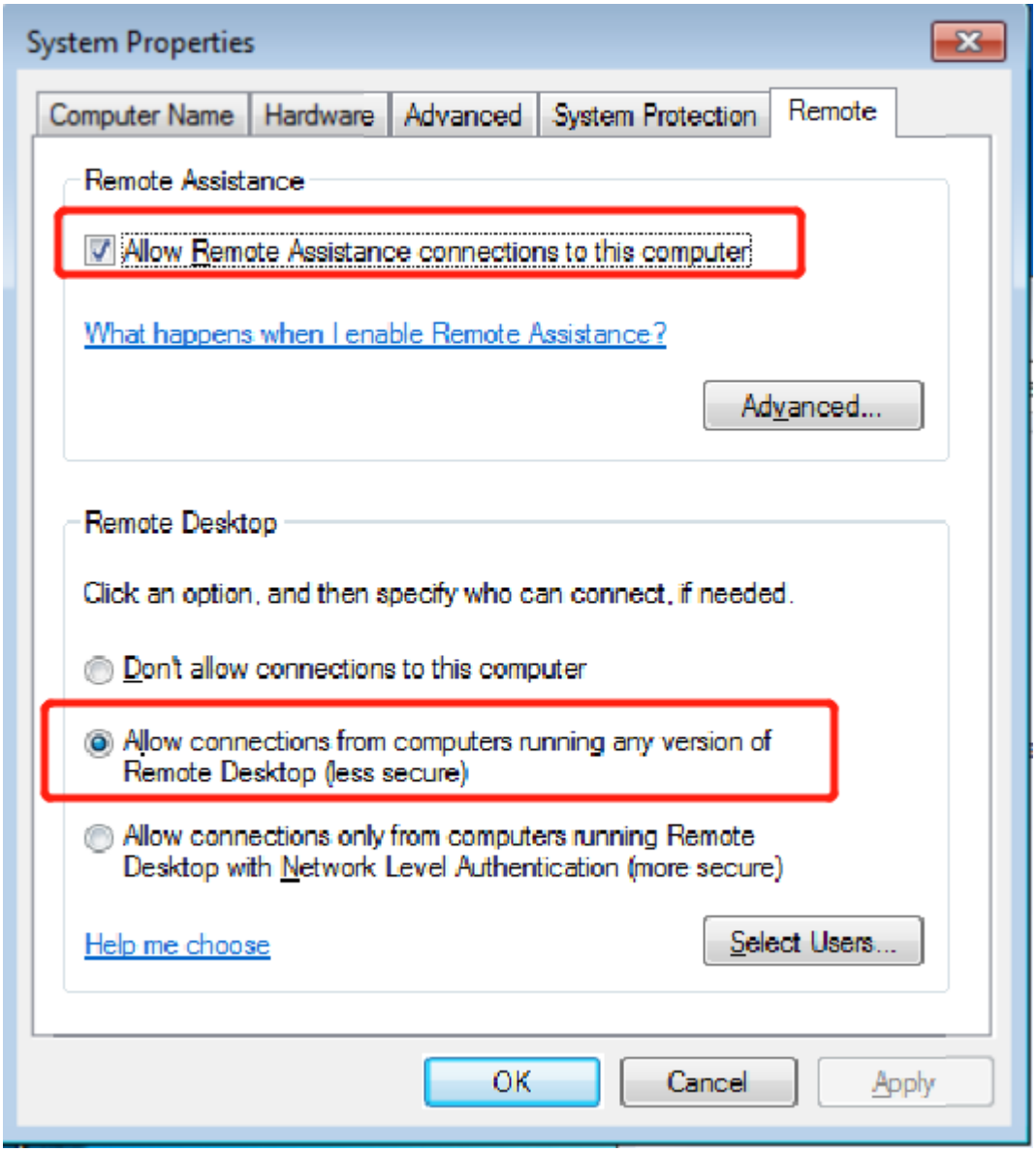
(1) Demonstrasi ini hanya berlaku ke pada klien yang dikondisikan secara virtualisasi atau komputer personal, dan selama demonstrasi keseluruhan pengetesan harus terisolasi dari network operasional, sehingga mencegah ransomware mengenkripsi komputer lainnya.

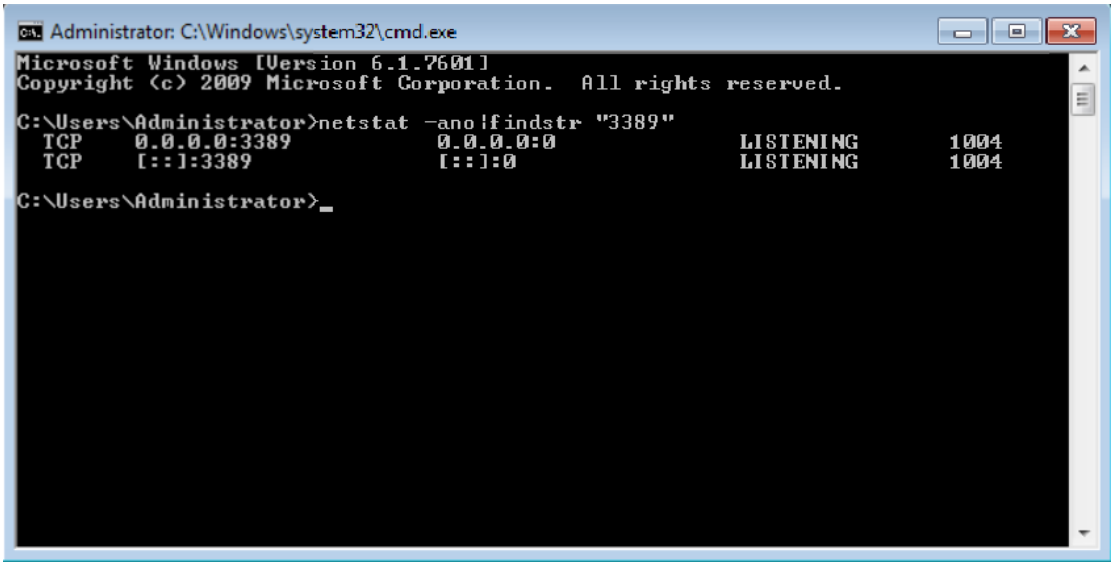
(2) Anda dapat mengatur MGR, PC 1, dan PC 2 sendiri. PC 1 dan PC 2 butuh diinstal agen Endpoint Secure.

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

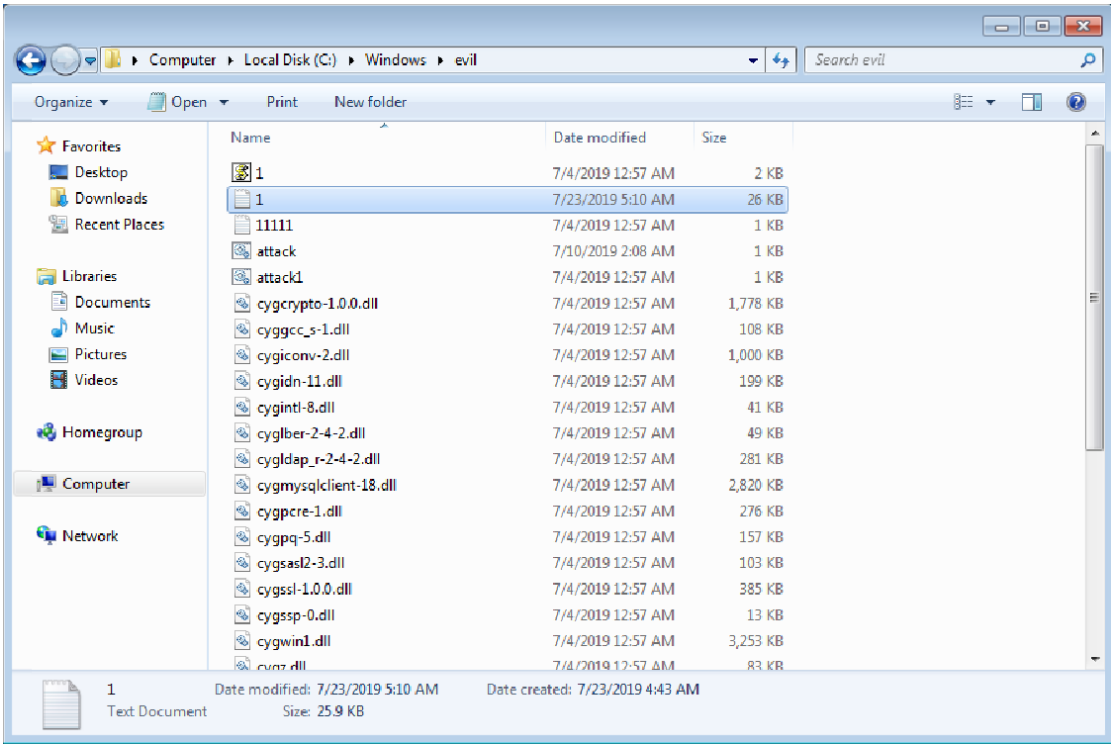
(4) PC 1 dan PC 2 dapat menggunakan alamat dari segment network 20.10.0.0/24. Program ransonware akan memindai secara otomatis PC lainnya yang berada di segment network yang sama.

(5) Anda dianjurkan untuk mematikan firewall windows dan mengaktifkan service RDP di PC 2 karena ransomware akan menyerang melalui port 3389 di PC 2.

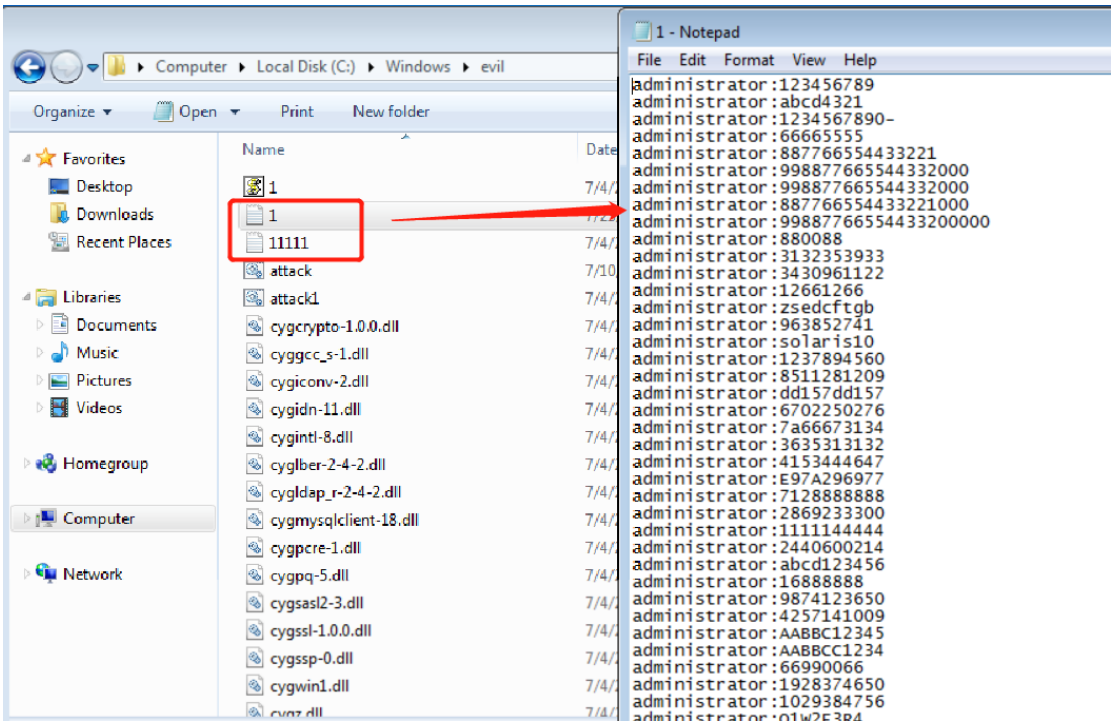




(6) Contoh ransomware butuh ditempatkan di direktori yang spesifik.



(7) Password yang digunakan virus untuk menyerang biasanya disimpan secara normal pada file text. Untuk itu, ketika and menggunakan system windows 7, pastikan bahwa password yang digunakan ada dalam text file (mengandung password nowmal) di alat virus. Direkomendasikan untuk menggunakan administrator/111111 sebagai username dan password.



2.5 Resiko

Resiko	Deskripsi
Mengisolasi semua yang terkait dengan proses demonstrasi	Sejak ransomware bekerja, demonstrasi akan dilakukan di lingkungan virtual dan perlu diisolasi dari network yang sebenarnya. Jika gagak, file dari komputer di jaringan akan terserang oleh ransomware.
Melakukan Snapshot di PC yang digunakan untuk demonstrasi	Selama demonstrasi, file PC akan terenkripsi oleh ransomware. Untuk segera mengembalikan status sebelumnya, anda memerlukan melakukan snapshoot di muka pada PC. .

Bagian 3 Proses Demonstrasi

3.1 Alur

3.1.1 Isi

Pada agen Endpoint Secure, aktifkan protection policy untuk PC 1 dan PC 2 (untuk mendeteksi dan memblok brute-force attack), dan proses demonstrasikan proses penyerangan dan efek dari ransomware.

3.1.2 Hasil yang Diharapkan

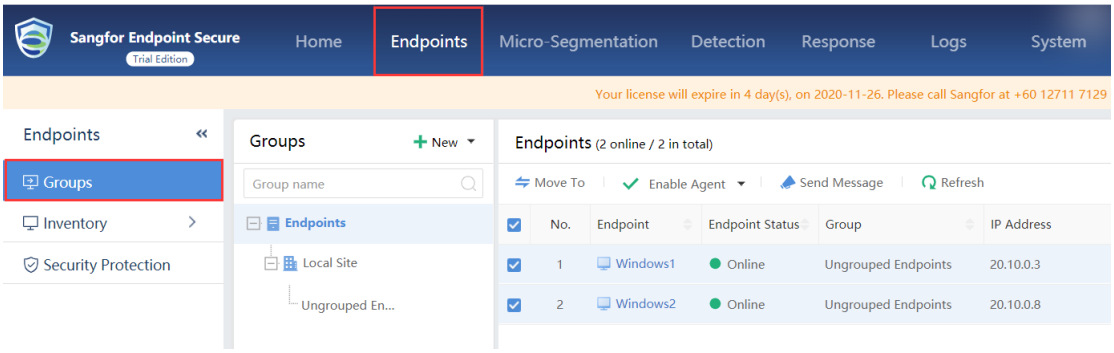
PC 1 dan PC 2 telah dilindungi oleh Endpoint Secure policy terhadap brute-force attacks, dimana memblok penyerangan dan penyebaran virus. Sebagai hasilnya, file tidak akan tereknripsi oleh ransomware.

3.1.3 Langkah

3.1.3.1 Mengembalikan Snapshots

(1) Roll back PC 1 dan PC 2 ke status sebelumnya saat snapshots

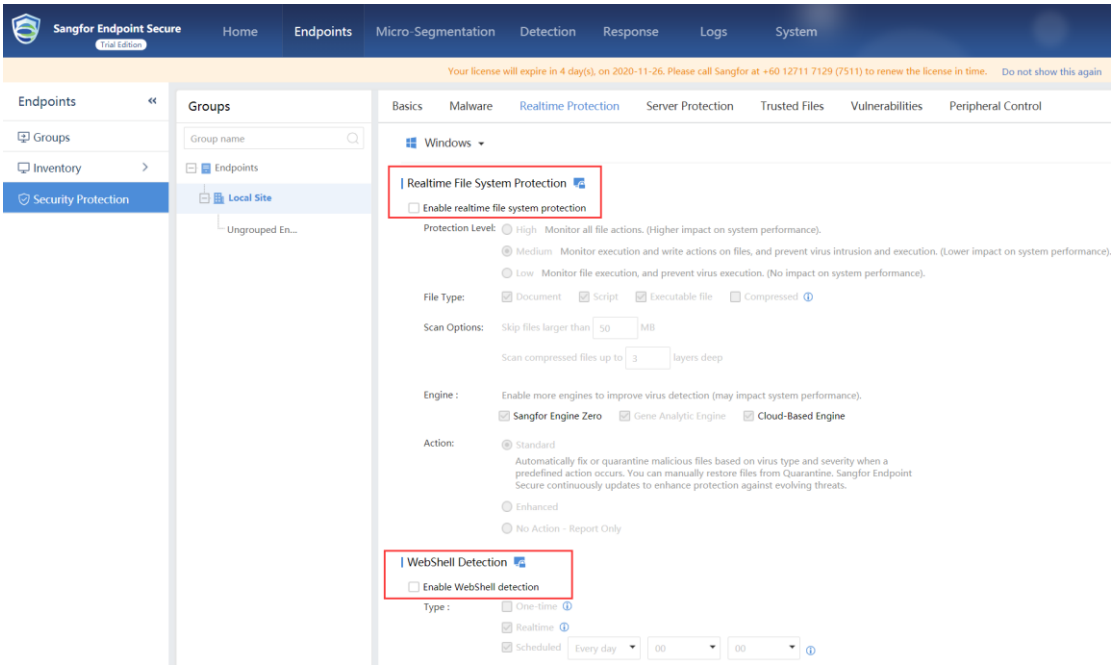
(2) Periksa MGR dan cari apakah kedua PC 1 dan PC 2 menjadi online, seperti terlihat dibawah:

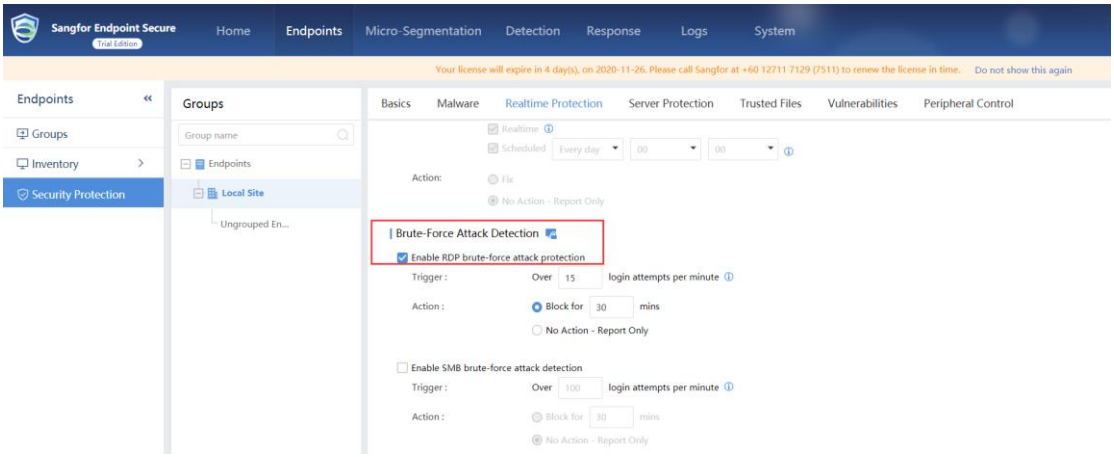


3.1.3.2 Pengaturan Policy

Aturlah security policy. Aktifkan policy untuk mendeteksi dan memblok brute-force attacks, dan nonaktifkan policy perlindungan real time lainnya.

Pilih **Endpoints** > **Security Protection**. Atur **Ungrouped Endpoints** policy (kedua PC 1 dan PC 2 menjadi online pada ungrouped endpoints secara default) dan pergilah ke **Realtime Protection** tab. Nonaktifkan real-time protection policy lainnya, seperti **Realtime File System Protection**, **Ransomware Protection**, dan **Advanced Threat Protection**. Nonaktifkan icon gembok. Aktifkan **RDP brute-force attack protection** dan periksa **Block for XX mins**, seperti ditunjukann dibawah:

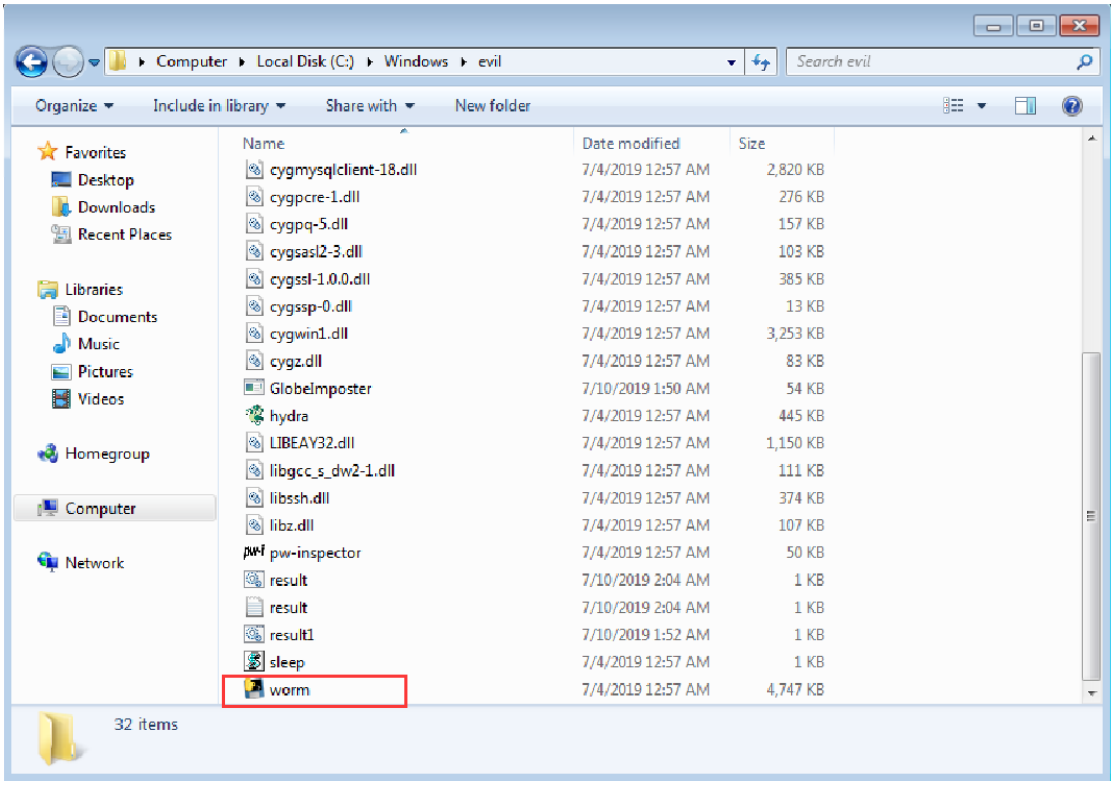




3.1.3.3 Penginisiasian Penyerangan

(1) Sebelum menginisiasi sebuah serangan, periksa status dari PC 1 dan PC 2. File komputer tersebut belum terkenkripsi dan dapat dibuka normal, seperti ditunjukkan dibawah:

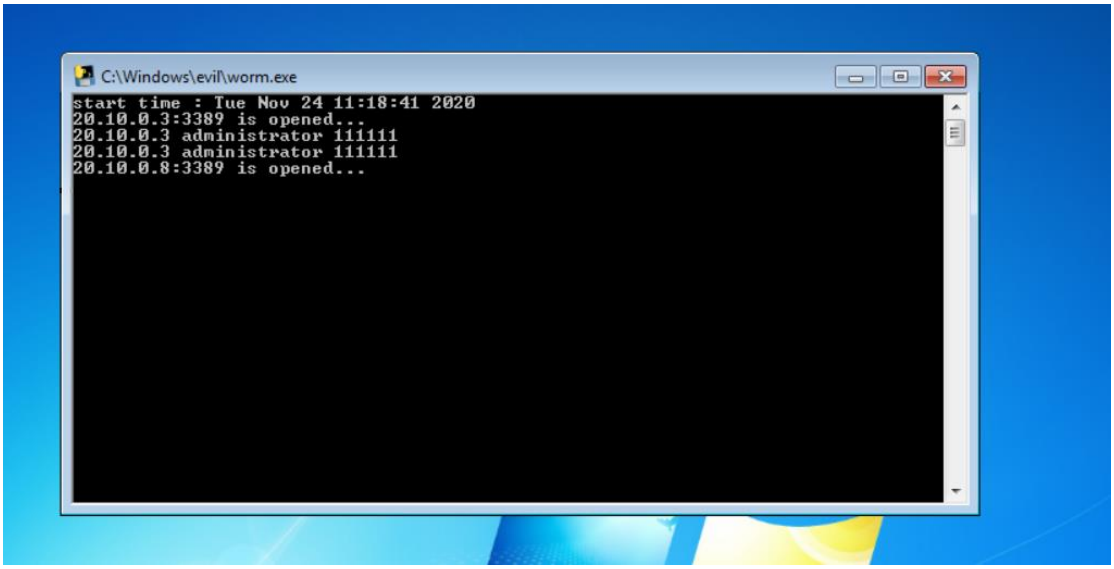
(2) Jalankan ransomware di PC 1, Seperti dibawah ini:



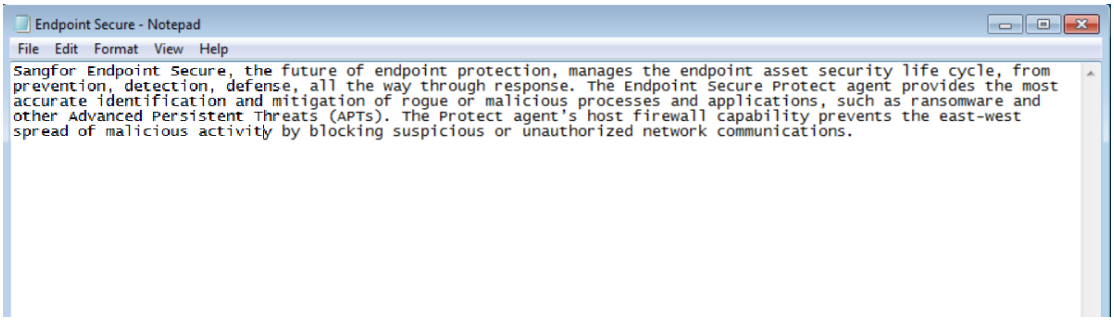
3.1.3.4 Efek Penyerangan

Virus akan menyerang dari PC 1 ke PC 2, dan menyebarkan ke LAN dan mengenkripsi file di PC 2. Pada tahap ini, Agen Endpoint Secure menjalankan policy against brute-force attacks untuk memblok celah serangan. Setelahnya, penyerangan virus gagal, dan file PC 1 dan PC 2 tidak terenkripsi. Anda dapat melihat log blok penyerangannya di Agen Endpoint Secure.

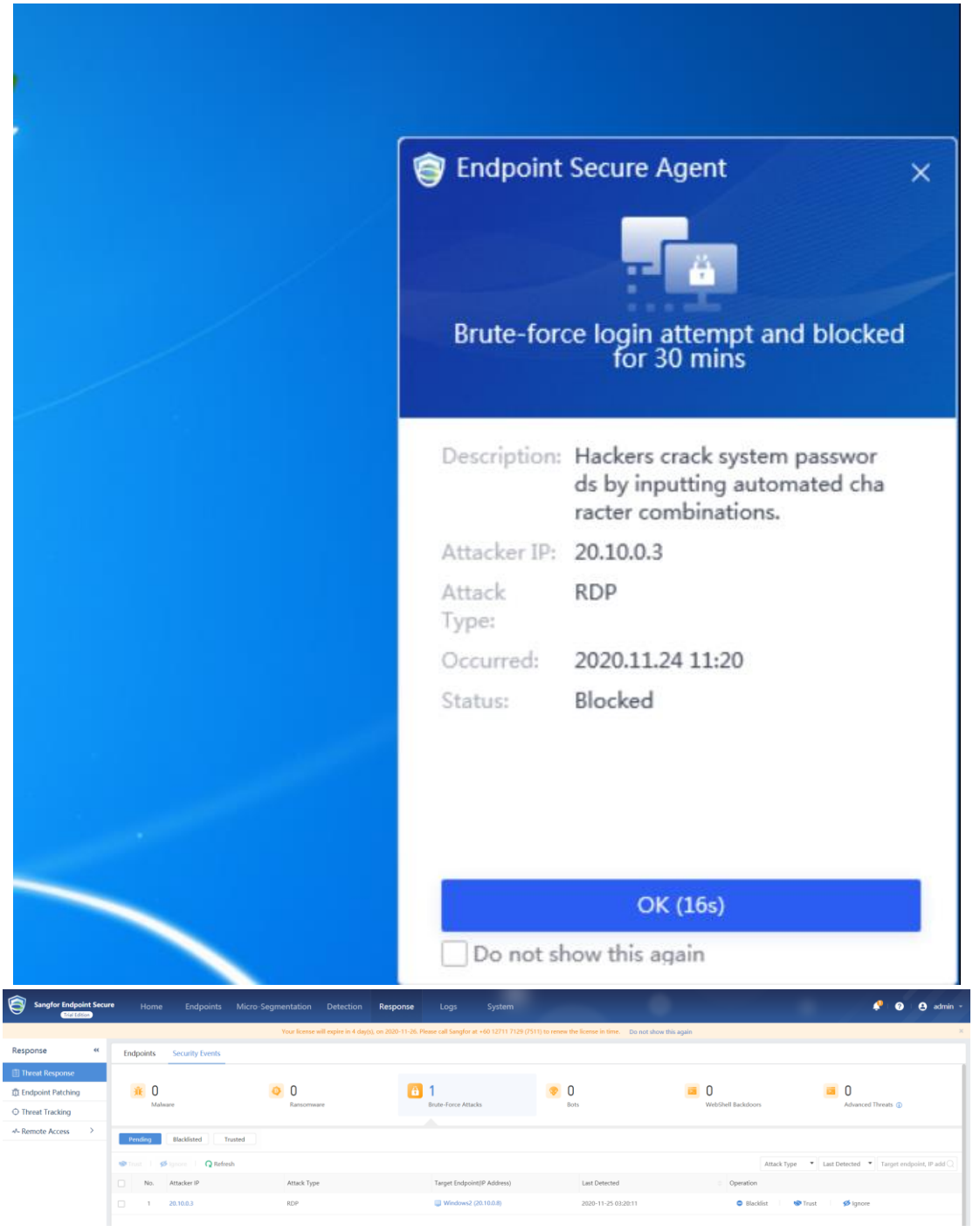
Log in di PC 1. Anda dapat menermuka penyerangan virus berhenti, seperti ditunjukan dibawah (sejak endpoint secure memblok penyerangan pada PC 2, virus tidak menyebar lebih lanjut.)



Periksa dan temukan file di kedua PC 1 dan PC 2 tidak terenkripsi. Lihat contoh di bawah:

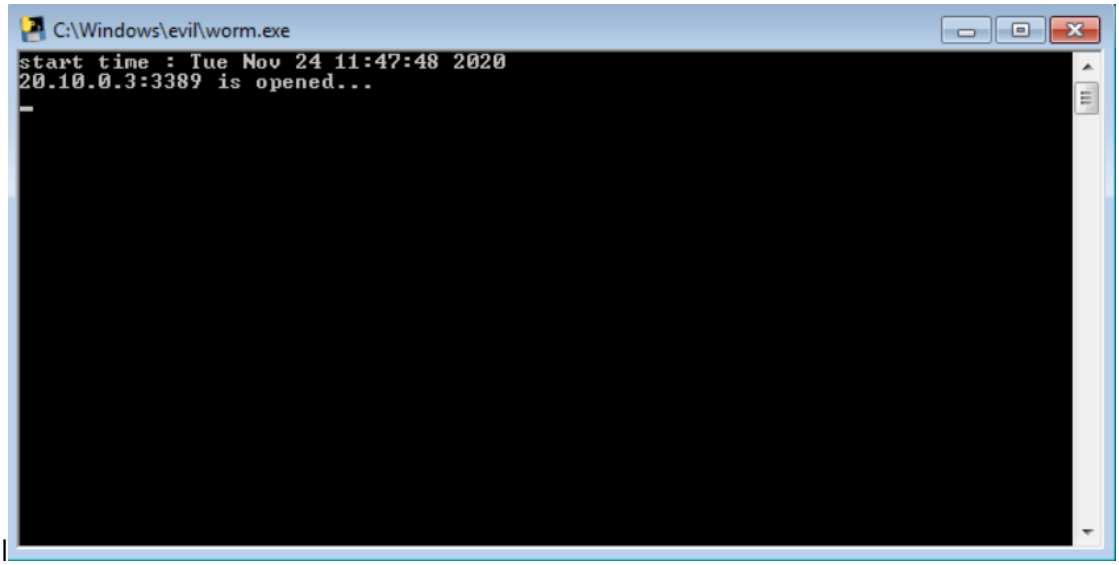


Lihat logs brute-force attacks di Agen Endpoint Secure. Pilih **Response** > **Threat Response** -> **Security Events** > **Brute-Force Attacks**. The brute-force attack terinisiasi melalui PC 1 dan telah sepenuhnya terblok, seperti ditunjukan dibawah :



Bagian 4 Pencegahan

1. Ketika program virus berjalan, sistem kemungkinan akan berhenti merespon beberapa kali dan tersangkut di posisi yang sama selama 2 menit. Pada kasus ini, anda harus menutup dan memulai kembali program.



2. Ambang penyerangan brute force

Ambang serangan RDP brute force

Mode pendeteksian cepat: mengkonfigurasi web console

Mode pendeteksian lambat : mode deteksi lamabat: 100 kali gagal login dalam 20 menit.

Pendistribusian deteksi: user yang sama gagal login di 8 IP berbeda dalam 60 detik.

Ambang serangan SMB brute force:

Mode pendeteksian cepat:konfigurasi di web console

Mode pendeteksian lambat: 200 kli gagal login dalam 20 menit.

Pendistribusian deteksi : user yang sama gagal login di 16 IP berbeda dalam 60 detik

SANGFOR