Praktik Terbaik Keamanan Endpoint untuk Skenario Menggunakan Mikrosegmentasi ke Anti Ransomware

Versi 3.2.22

Catatan Perubahan

Tanggal	Change Description
25 Februari 2021	Dokumen diterbitkan
17 Mei 2021	Dokumen diperbaharui

DAFTAR ISI

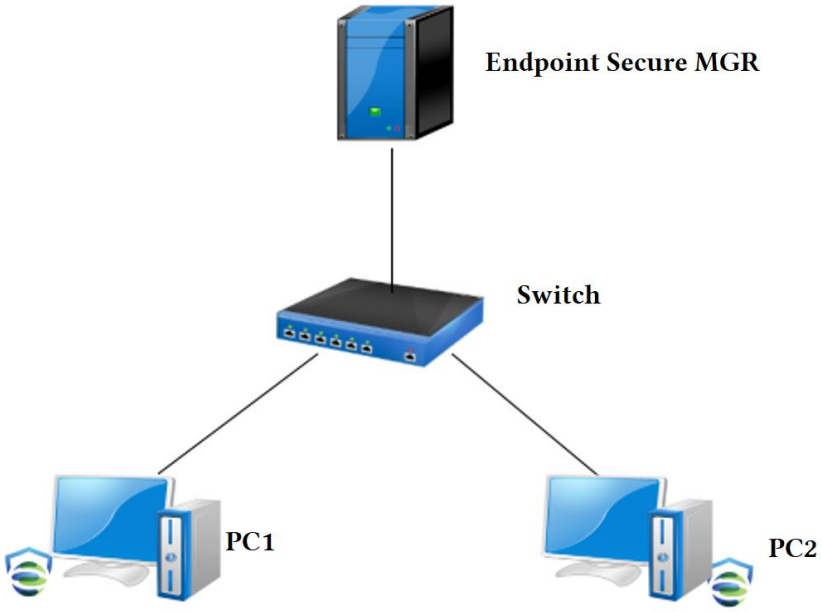
Bagian 1 Gambaran

Program ini mendemonstrasikan proses dan efek dari penyerangan ransomware ketika tidak menjalankan Endpoint Secure Agent, kemudian efek pendeteksian dan perlindungan terhadap ransomwre setelah menggunakan Endpoint Secure Agent. Hal ini sangat sesuai untuk menunjukkan kepada pelanggan bagaimana Endpoint Secure Agent mendeteksi serangan ransomware dan menyediakan perlindungan.

Bagian 2 Persiapan untuk Demonstrasi

2.1 Lingkungan

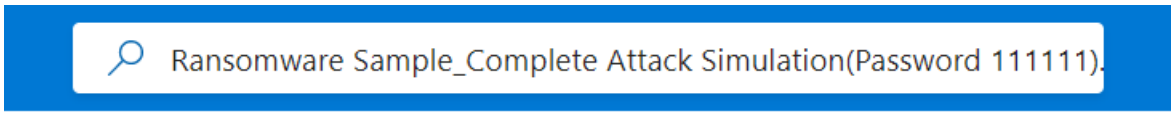
2.1.1 Lingkungan Network

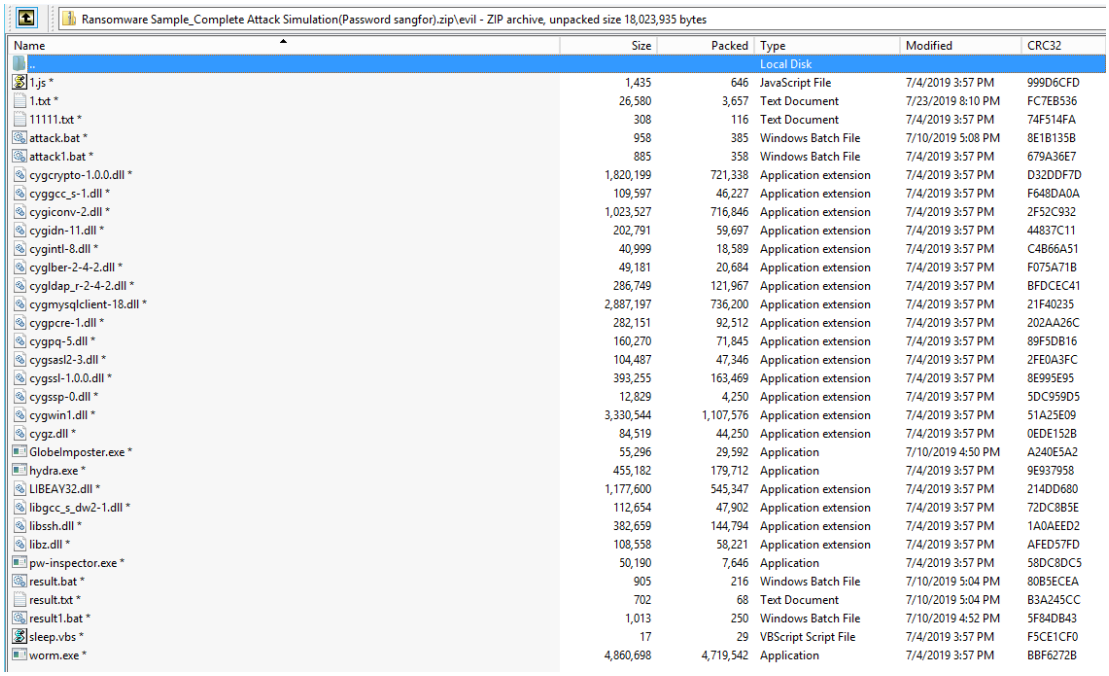


Perangkat	Akun/Password	IP	Deskripsi
PC1	administrator/111111	20.10.0.3	PC imenginisiasi penyerangan ransomware
PC2	administrator/111111	20.10.0.8	PC diserang oleh ransomware menggunakan RDP brute-force cracking
MGR	admin/Endpoint Secure@support	20.10.0.100	Endpoint Secure MGR

2.1.2 Contoh Virus

Untuk menyimulasikan prose penyerangan, anda dapat mengunduh **Ransomware Sample_Complete Attack Simulation(Password 111111).zip** pada PMO




Ransomware Sample_Complete Attack Simulation(Password sangfor).zip\evil - ZIP archive, unpacked size 18,023,935 bytes

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
cygldap-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 pada C:/windows/evil of PC 1. Selama serangan, virus akan mulai menyerang PC 2 yang berada di LAN yang sama via RDP brute-force attack. Setelah penyerangan komplit, file komputer di lokal PC,sama dengan file pada PC 2 akan terenkripsi.

2.3 Konten

Tahap	Konten	Hasil Yang Diharapkan
Ronde 3	Pada Endpoint Secure MGR, aktifkan protection policy untuk PC 1 dan PC 2 (mengaktifkan micro-segmentation policy untuk memblok sharing ports), dan mendemonstrasikan proses penyerangan dan efek ransomware.	1. File pada PC 1 terekripsi oleh ransomware. 2. PC 2 terlindungi oleh micro-segmentation policy dari Endpoint Secure, dimana memblok celah dan penyebaran virus. Hasilnya, file tidak terenkripsi oleh

		ransomware.

2.4 Deskripsi

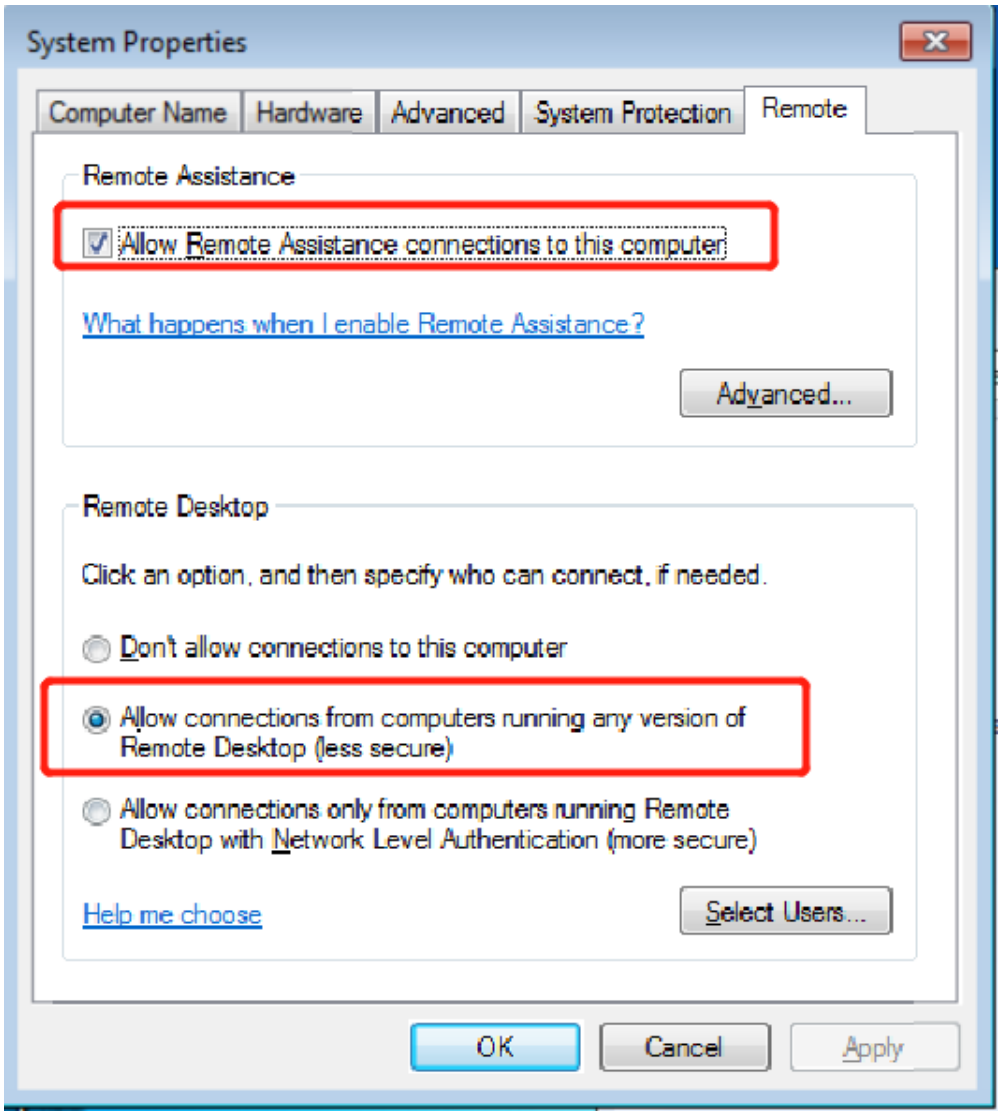
(1) Demonstrasi ini hanya berlaku pada lingkungan virtual dan diterapkan pada klien atau komputer perorangan, dan lingkungan demonstrasi ini harus diisolasi dari network bisnis pelanggan, sehingga mencegah ransomware mengekripsi komputer lainnya.

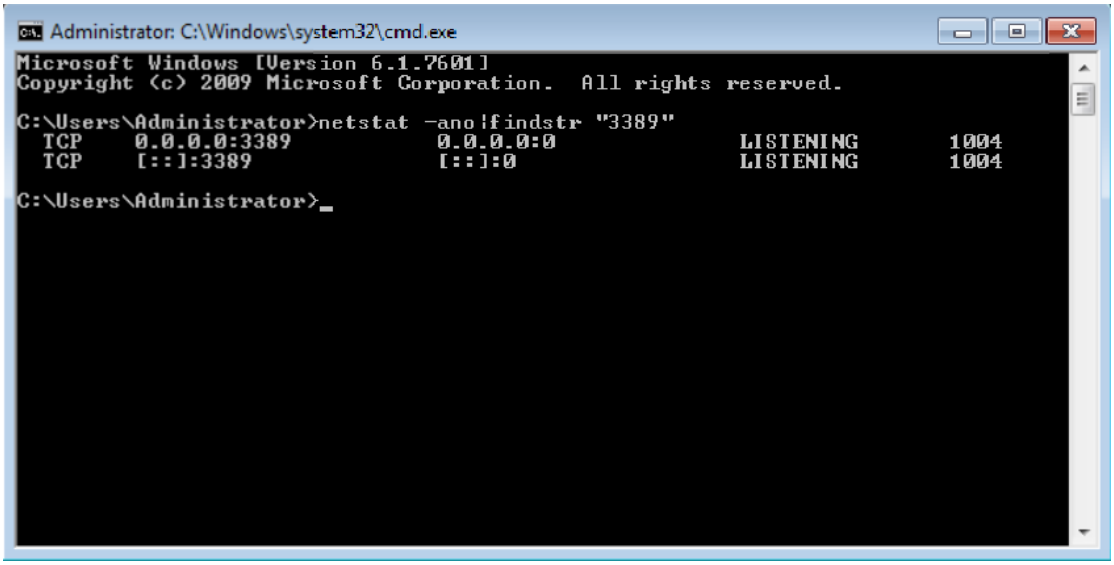
(2) Anda dapat mengatur MGR, PC 1, dan PC 2 oleh diri and sendiri. PC 1 dan PC 2 butuh diinstall Endpoint Secure Agent.

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

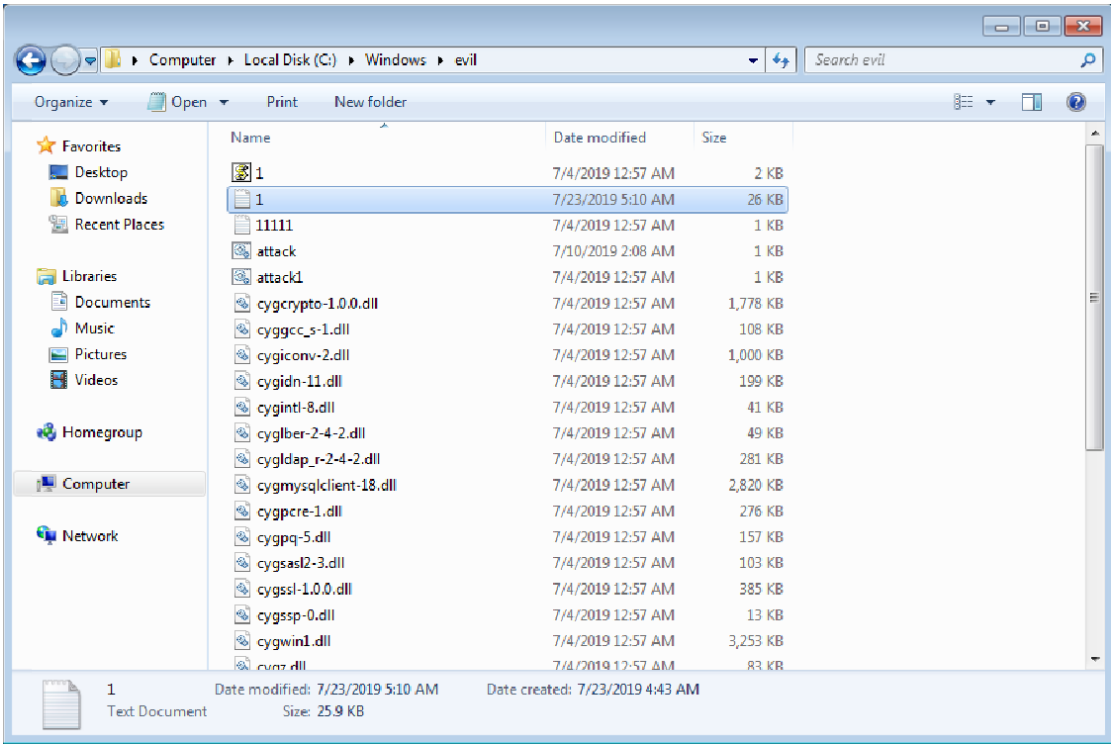
(4) PC 1 dan PC 2 dapat menggunakan alamat segment network 20.10.0.0/24. Ransomware secara otomatis akan memindai pc yang berada pada segment network yang sama.

(5) Anda disarankan mematikan system firewall pada Windows dan mengaktifkan RDP service pada PC 2 dimana ransomware akan menyerang melalui port 3389 pada PC 2.

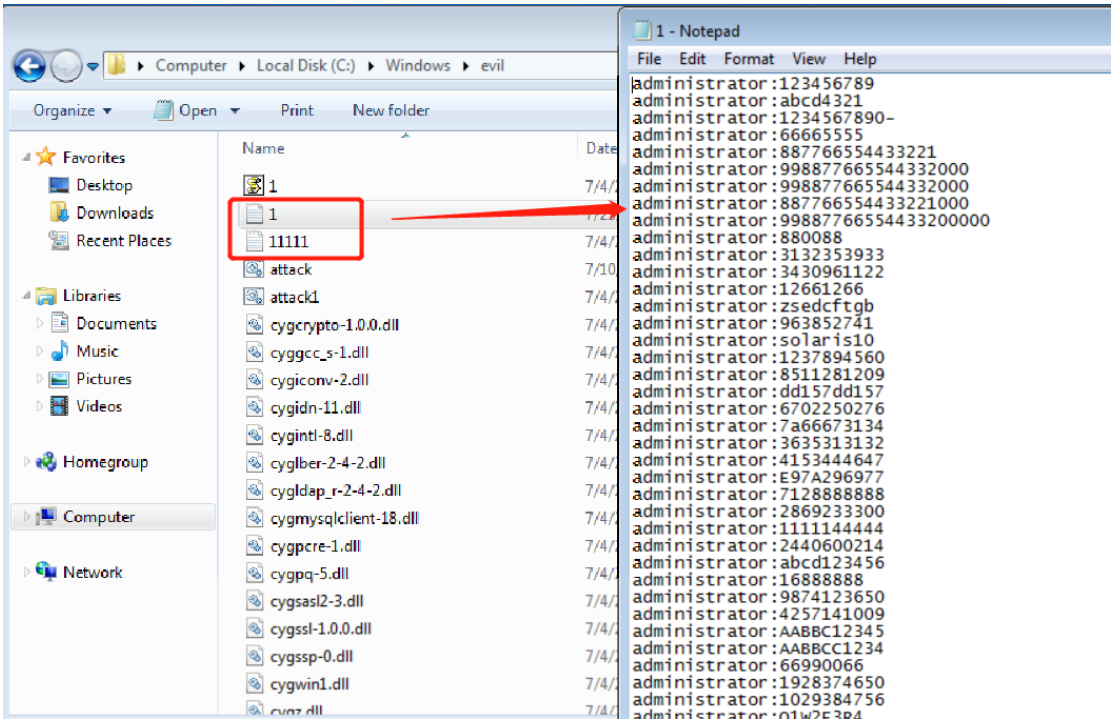




(6) Contoh ransomware butuh ditempatkan di tempat spesifik.



(7) Password yang digunakan oleh virus biasanya disimpan pda file text. Karena itu, ketika menggunakan Windows 7 system anda, pastikan password tercover oleh text (mengandung password umum) pada peralatan virus. Direkomendasikan menggunakan administrator/111111 sebagai username dan password.



2.5 Resiko

Resiko	Deskripsi
Isolasi lingkungan demonstrasi	Sejak ransomware is berjalan, demonstrasi akan dilakukan pada lingkungan virtual dan butuh diisolasi dari network yang sebenarnya. Jika gagal melakukan seperti ini, maka file dari komputer lain akan diserang oleh ransomware.
Snapshot pada PC yang diguakan untuk demonstrasi	Selama demonstrasi, file pc akan terenkripsi oleh ransomware, Untuk lebih cepat mengembalikan kondisi sebelumnya untuk demonstrasi selanjutnya, anda butuh snapshot PC terlebih dahulu.

Bagian 3 Proses Demonstrasi

3.1 Ronde 3

3.1.1 Konten

Pada Endpoint Secure MGR, aktifkan protection policy pada PC 1 dan PC 2 (mangaktifkan the micro-segmentation policy untuk memblok haring ports), dan demonstrasikan proses

dan efek penyerangan ransomware.

3.1.2 Hasil Yang Diharapkan

(1) File PC 1 terenkripsi oleh ransomware.

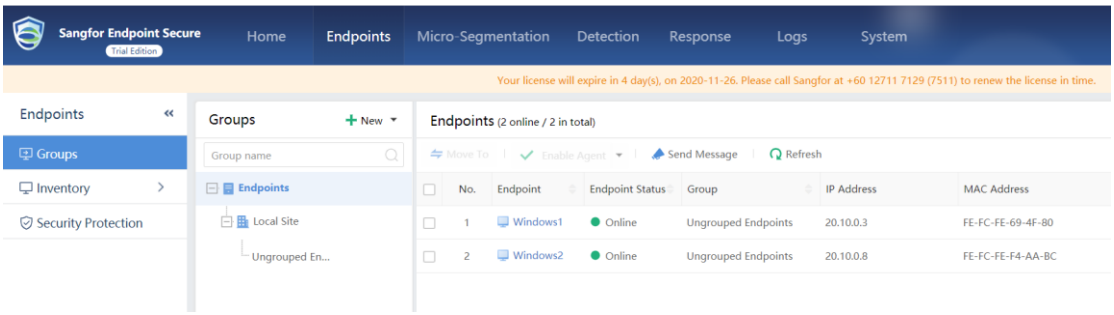
(2) File PC 2 dilindungi oleh micro-segmentation policy dari Endpoint Secure, dimana memblok penyebaran dan serangan virus. Sebagai hasilnya file tidak terenkripsi oleh ransomware.

3.1.3 Langkah Langkah

3.1.3.1 Mengembalikan dari Snapshots

(1) Pengembalian PC 1, PC 2, dan Endpoint Secure MGR ke kondisi sebelumnya menggunakan snapshot.

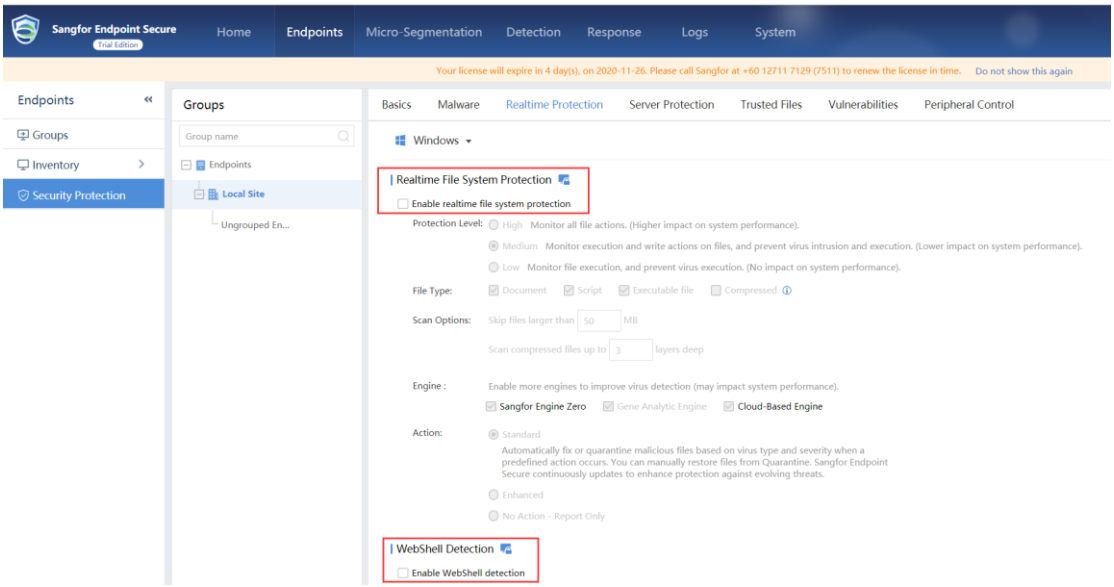
(2) Periksa Endpoint Secure MGR dan temukan bahwa kedua PC 1 dan PC 2 menjadi online, seperti ditunjukkan dibawah:

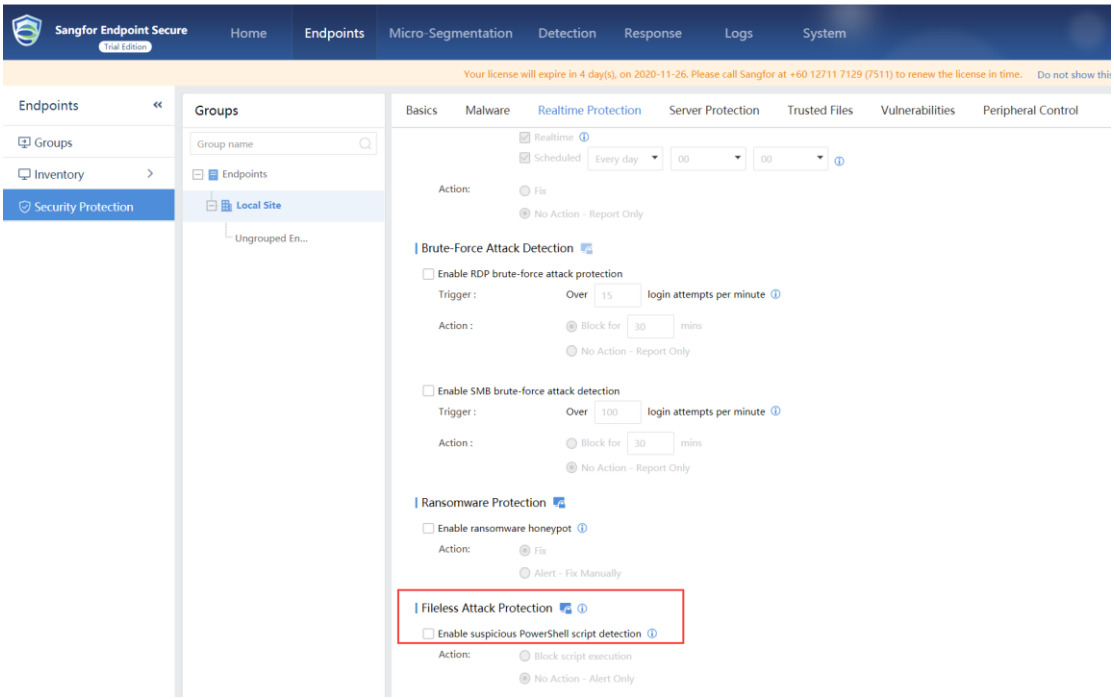


3.1.3.2 Pengaturan Policy

(1) Nonaktifkan semua real-time protection policies.

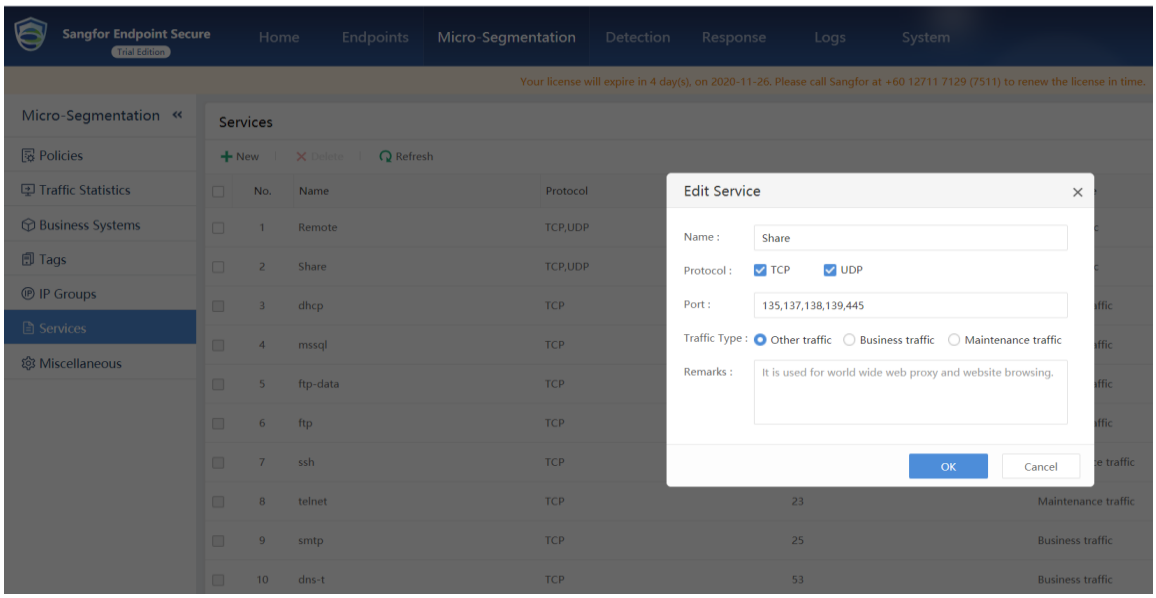
Seperti ditunjukkan dibawah, pilih **Endpoints** > **Security Protection**. Atur **Ungrouped Endpoints** policy lalu pergi ke tab **Realtime Protection**. Nonaktifkan **Realtime File System Protection**, **Ransomware Protection**, **Advanced Threat Protection**, **WebShell Detection**, dan **Brute-Force Attack Detection**. Hidupkan icon gembok.

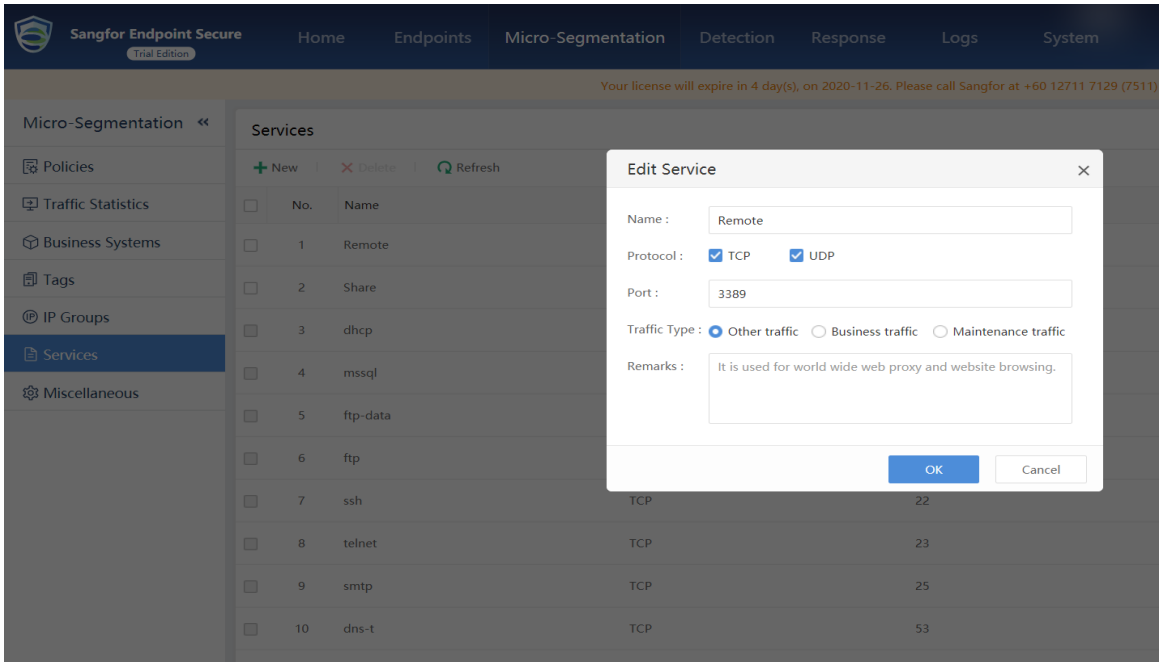




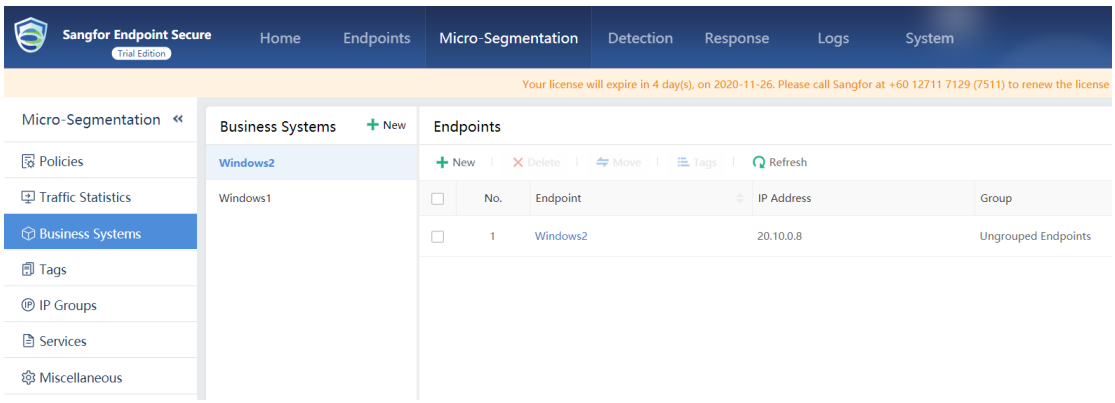
(2) Atur micro-segmentation policy untuk menolak akses berbagi port dan tolak akses sharing ports dan remote desktop di PC 2.

Tentukan service sharing port,.seperti ditunjukkan dibawah, pilih **Micro-Segmentation** > **Services**. Sharing ports termasuk 135, 137, 138, 139, dan 445, dan port remote desktop adalah 3389

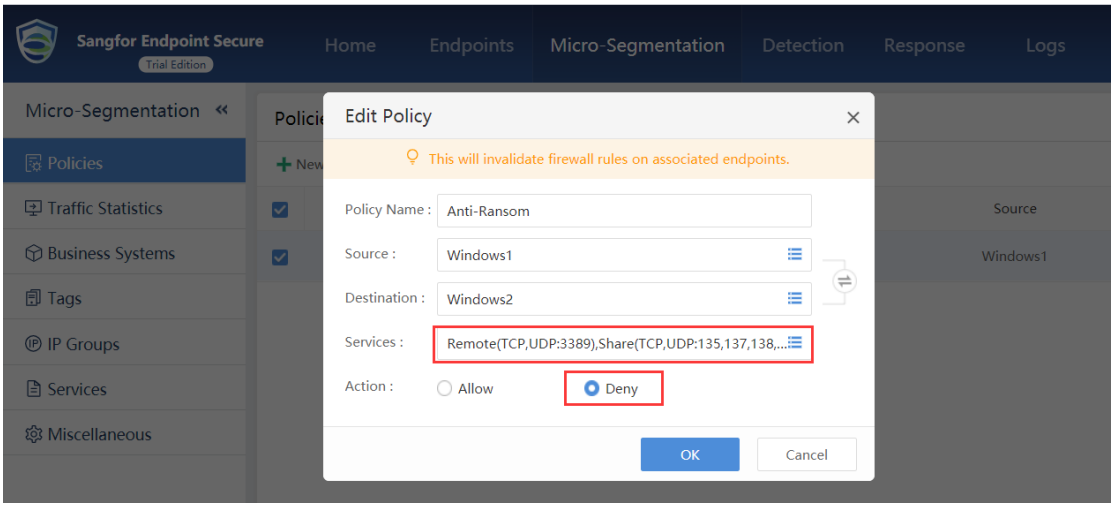




Tetapkan business systems PC 1 dan PC 2. Pilih **Micro-Segmentation** > **Business Systems**, seperti dibawah ini.

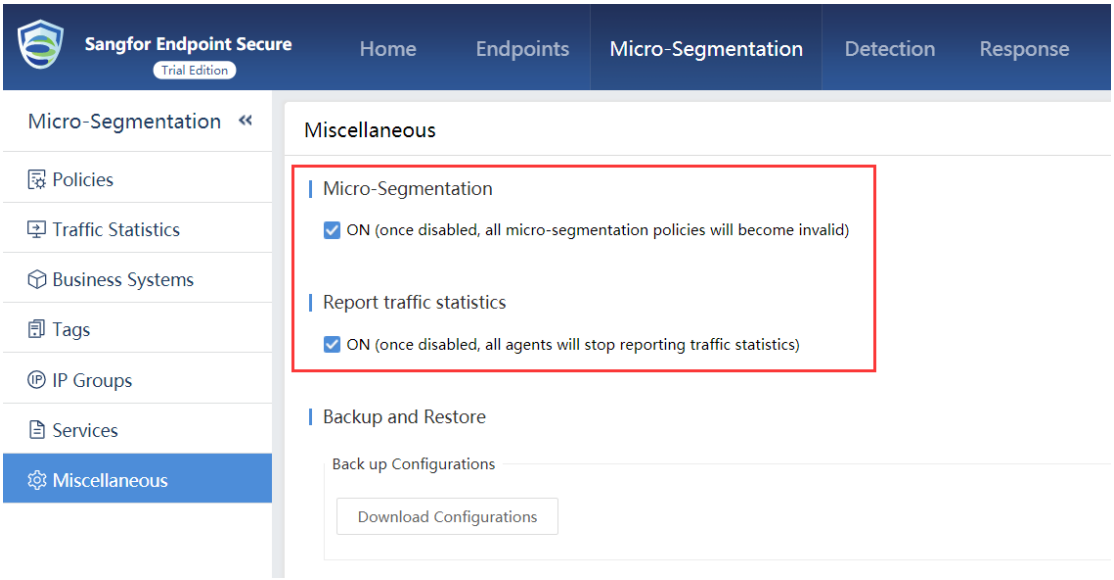


Tetapkan micro-segmentation policy memblok sharing port, seperti ditunjukkan dibawah, untuk menolak PC1 akses untuk sharing port dan remote desktop port di PC 2.



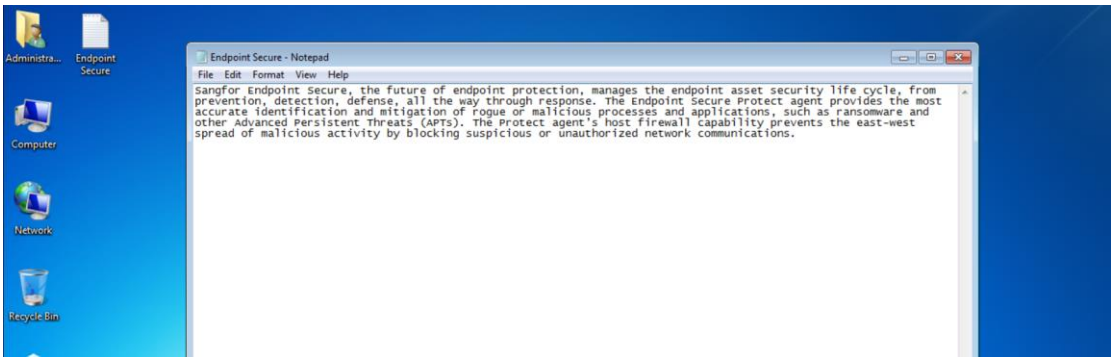
Aktifkan Micro-Segmentation dan Report traffic statistics. Seperti ditunjukkan dibawah, pilih

Micro-Segmentation > **Miscellaneous**.

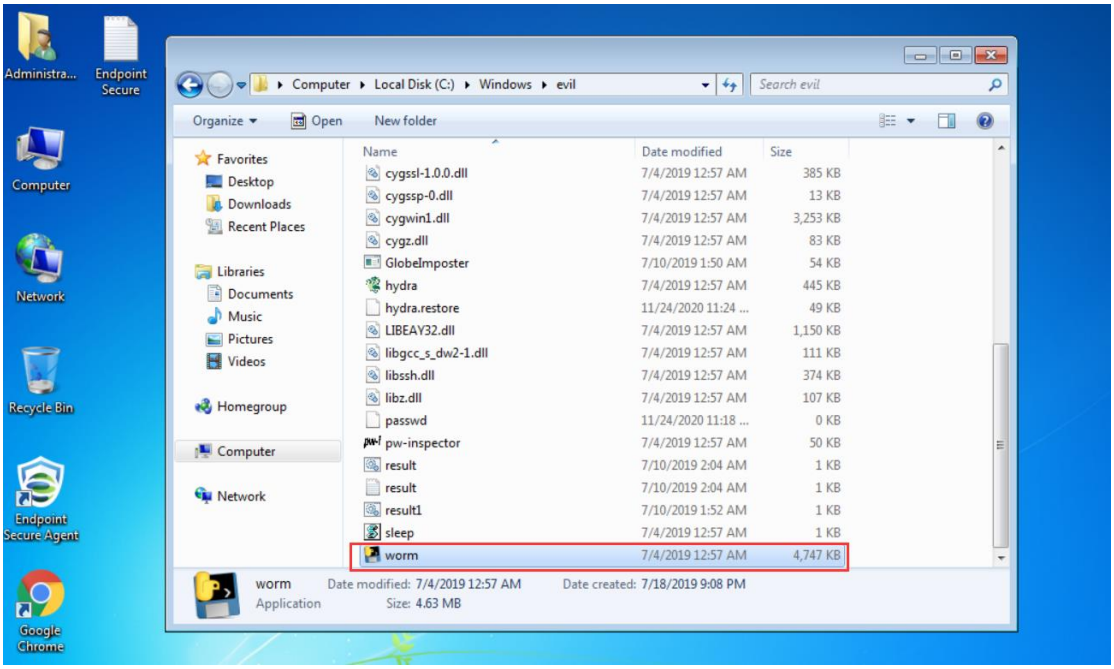


3.1.3.3 Menginisiasi Penyerangan

(1) Sebelum menginisiasi sebuah penyerangan, periksa status check di PC 1 dan PC 2. File komputer mereka tidak terenkripsi dan dapat dibuka secara normal, seperti ditunjukkan dibawah:



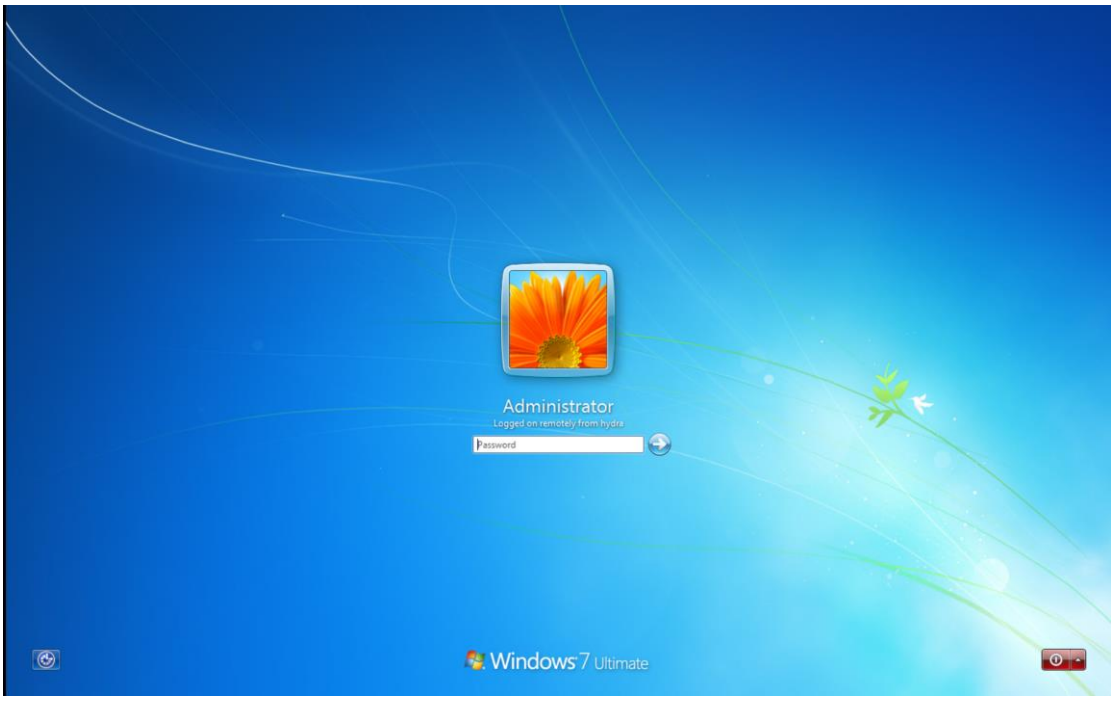
(2) Jalankan ransomware (Siapkan di lingkungan OVA) di PC 1, seperti ditunjukkan dibawah:



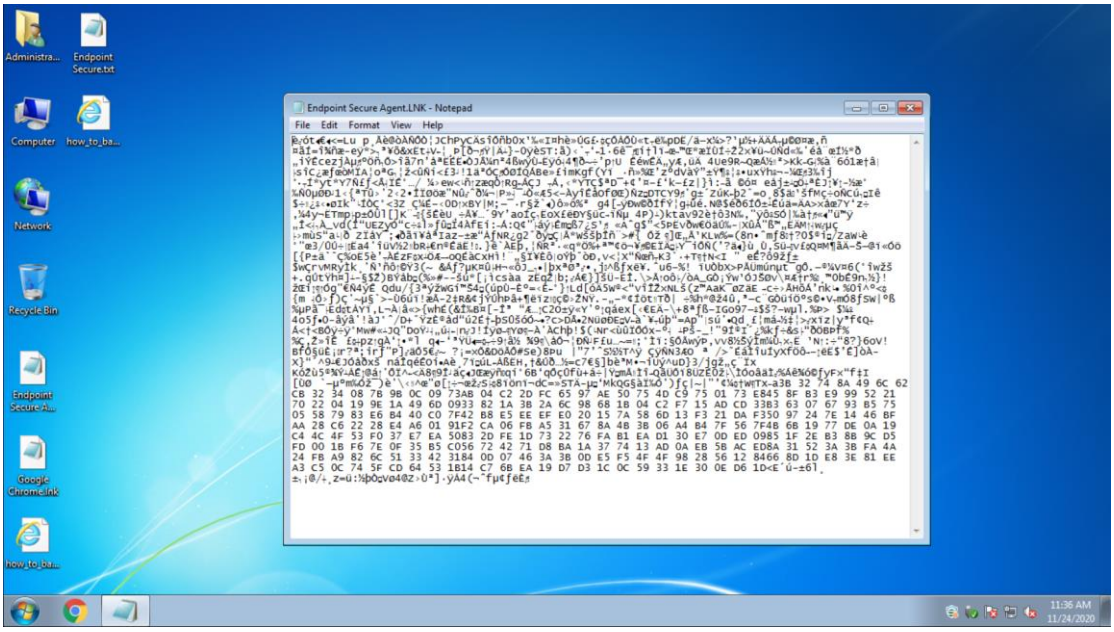
3.1.3.4 Efek Penyerangan

Penyerangan bertahanan 2 sampai 5 menit. PC 1 disserang, dan file di PC 1 terenkripsi, Untuk PC2, micro-segmentation policy memblok sharing port untuk mencegah serangan, dan file di PC 2 tidak terenkripsi oleh ransomware.

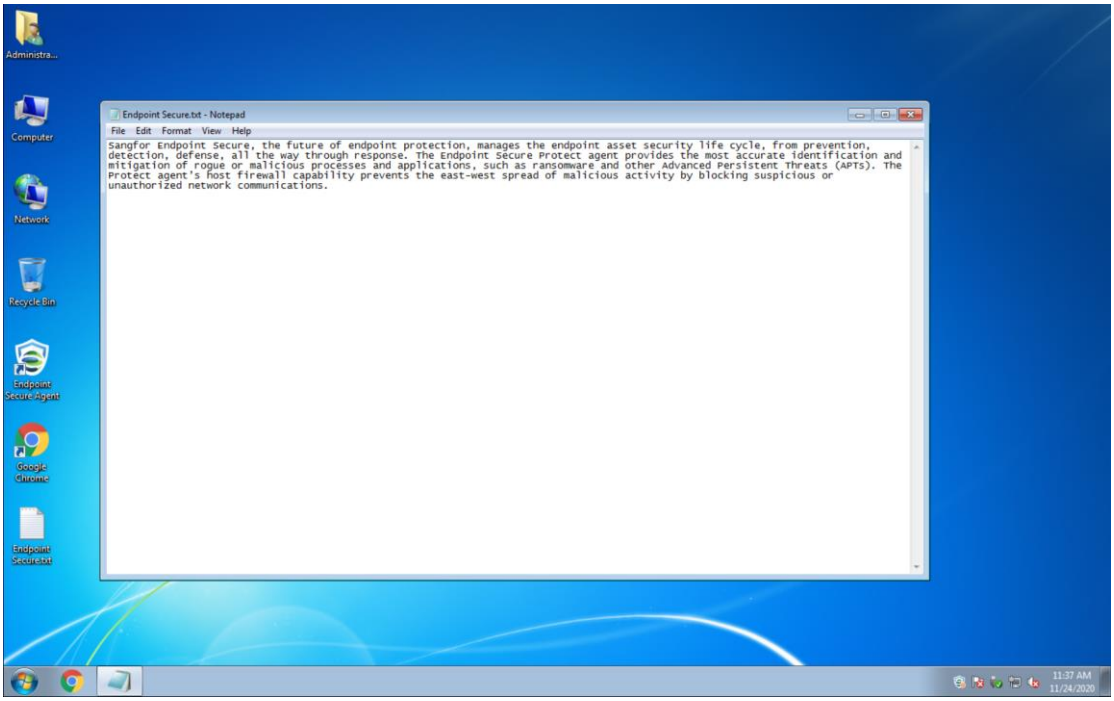
Setelah menjalankan ransomware, PC 1 telah terserang, keluar dan masuk kembali menggunakan administrator/111111, seperti ditunjukkan dibawah:



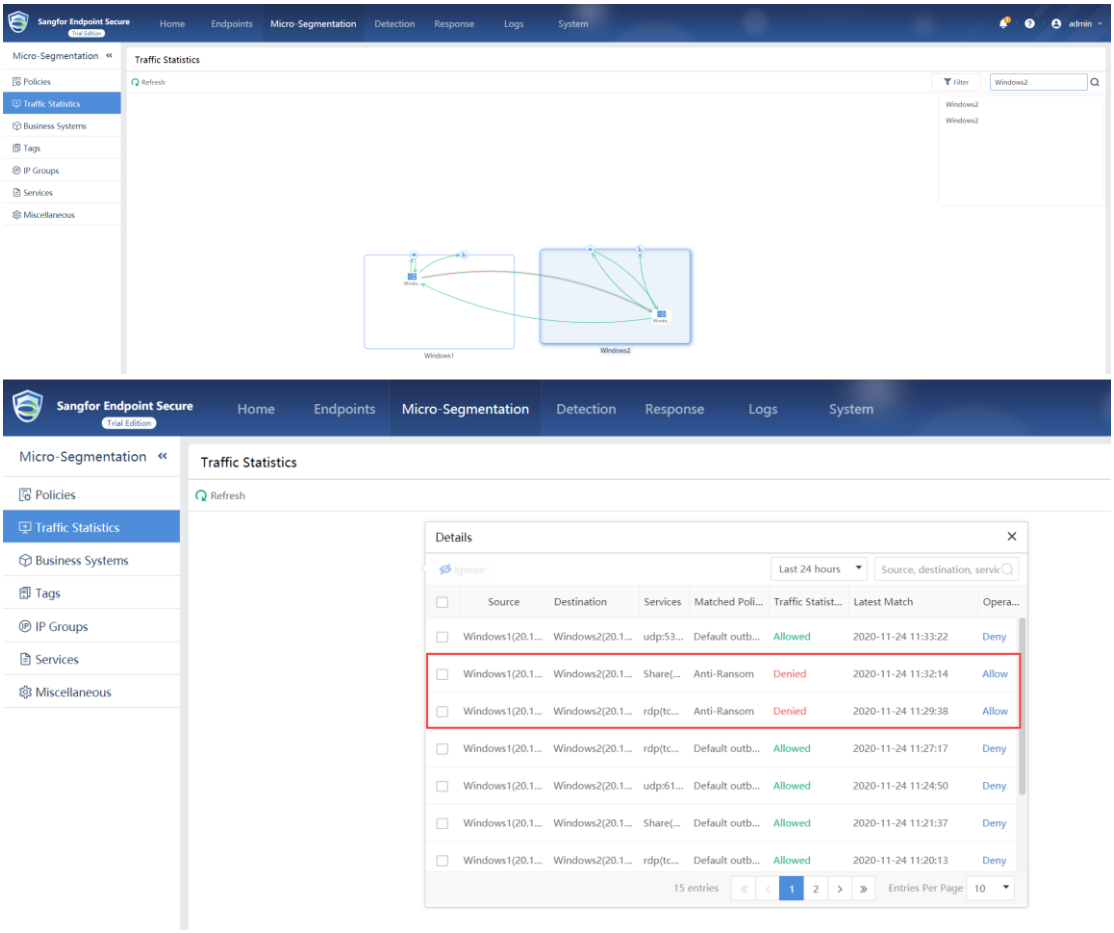
PC 1 menjalankan ransomware, dan file pada komputer PC 1 terenkripsi, seperti ditunjukkan dibawah:



Untuk PC 2, micro-segmentation policy memblok sharing ports untuk menhentikan serangan, dan file komputer pada PC 2 tidak terenkripsi oleh ransomware, Lihat figur dibawah:

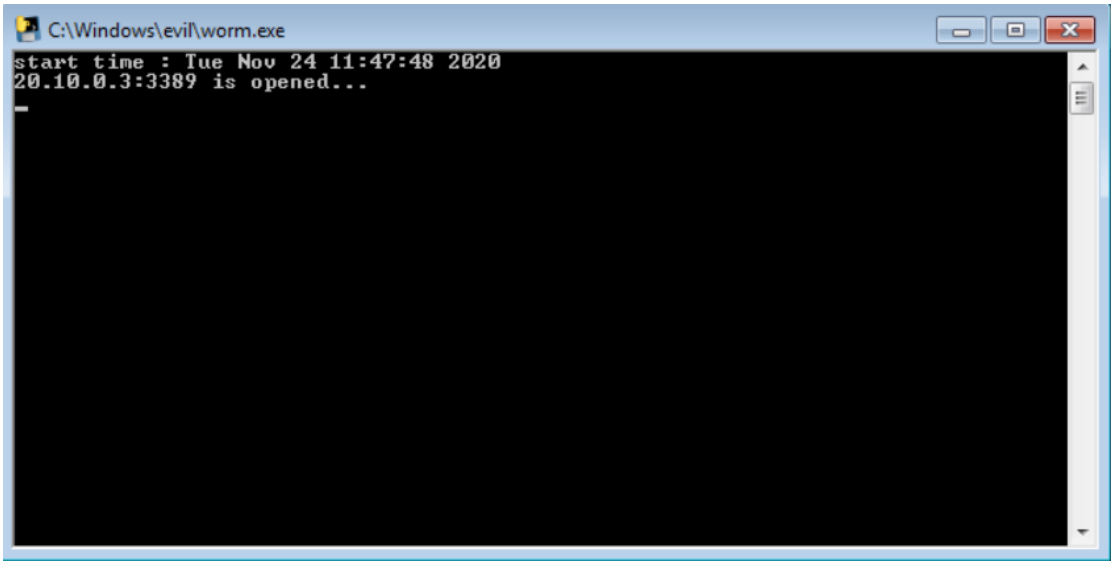


Lihat trafik catatan pada of micro-segmentation. Pilih **Micro-Segmentation** > **Traffic Statistics**. Klik PC 2 dan lihat akses recordnya. Anda dapat menemukan bahwa akses sharing ports PC 1 tke PC 2 telah ditolak, seperti ditunjukkan gambar dibawah:



Bagian 4 Himbauan

1. Ketika program virus berjalan, system mungkin akan berhenti merespon beberapa kali dan akan terdiam dalam posisi dibawah selama 2 menit. Pada kasus ini, anda harus menutup dan mejalankan ulang program.



SANGFOR