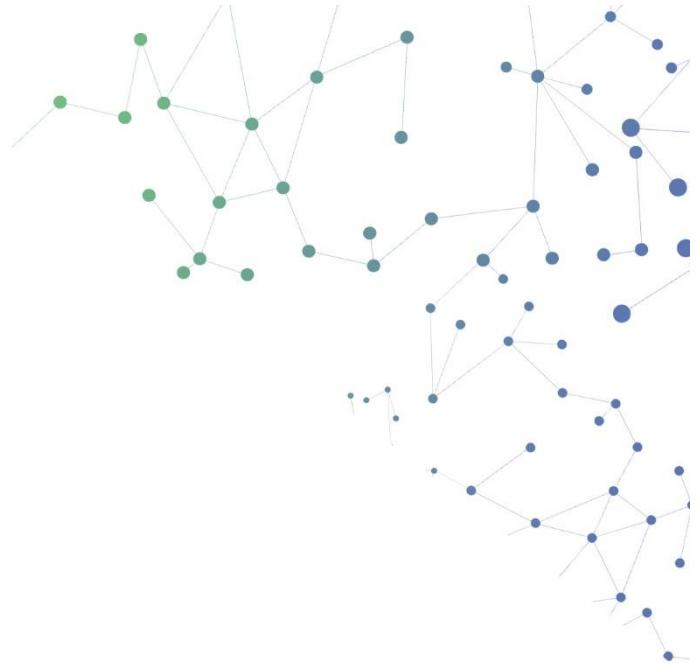


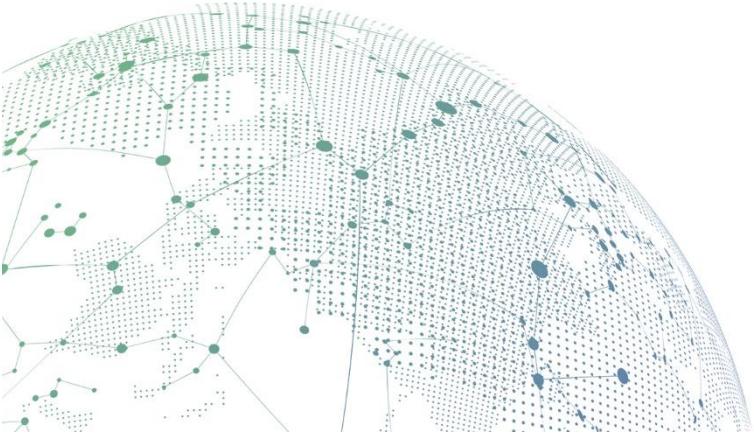


SANGFOR



Praktik Terbaik Keamanan Endpoint untuk Skenario Menggunakan Honeypot untuk Anti Ransomware

Versi 3.2.22



Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Februari 2021	Dokumen diterbitkan
17 Mei 2021	Dokumen diperbaharui

DAFTAR ISI

Bagian 1 Gambaran	1
Bagian 2 Persiapan untuk Demonstrasi	1
2.1 Kondisi	1
2.1.1 Kondisi Network.....	1
2.2 Proses Penyerangan.....	2
2.3 Konten.....	2
2.4 Deskripsi	3
2.5 Resiko.....	5
Bagian 3 Proses Demonstrasi.....	6
3.1 Alur	6
3.1.1 Konten.....	6
3.1.2 Hasil yang diharapkan	6
3.1.3 Langkah Langkah	6
3.1.3.1 Mengembalikan dari Snapshots.....	6
3.1.3.2 Pengaturan Policy	7
3.1.3.3 Menginisiasi Penyerangan	8
3.1.3.4 Efek Penyerangan	9
Bagian 4 Anjuran.....	11

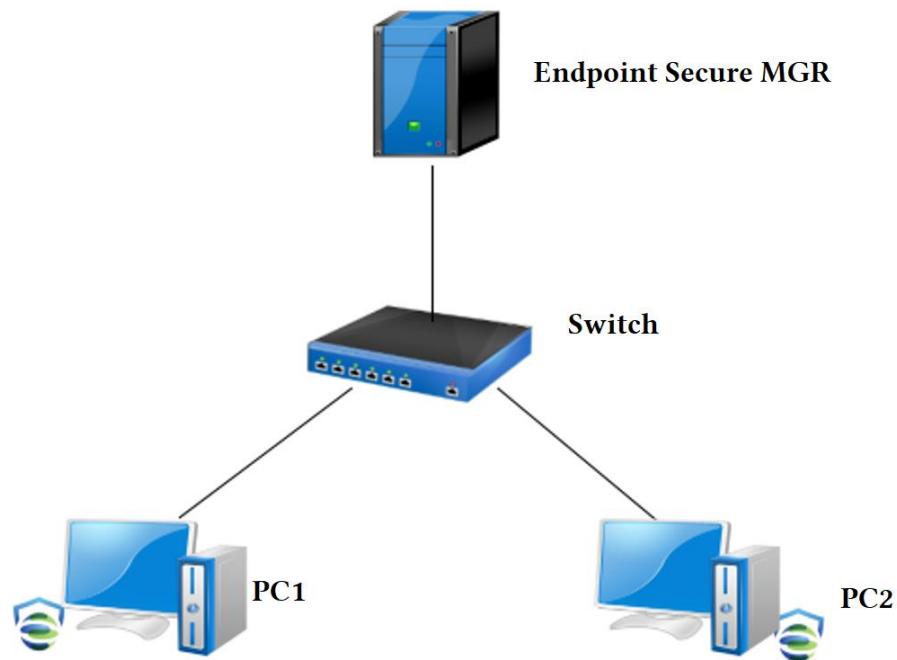
Bagian 1 Gambaran

Program ini mendemonstrasikan proses dan efek dari ransomware ketika sebuah endpoint tidak menjalankan agen Endpoint Secure, dan juga efek pendekripsi dan perlindungan kepada ransomware setelah memasang Agen Endpoint Secure. Ini sangat cocok untuk menunjukkan kepada pelanggan bagaimana Agen Endpoint Secure mendekripsi serangan ransomware dan menyediakan perlindungan.

Bagian 2 Persiapan untuk Demonstrasi

2.1 Kondisi

2.1.1 Kondisi Network



Perangkat	Akun/Password	IP	Deskripsi
PC1	administrator/111111	20.10.0.3	PC menginisiasi penyerangan ransomware
PC2	administrator/111111	20.10.0.8	PC terserang oleh ransomware dengan celah RDP brute-force

Use Honeypot to Anti Ransomware

MGR	admin/Endpoint Secure@support	20.10.0.100	Endpoint Secure MGR
-----	----------------------------------	-------------	---------------------

Untuk melakukan simulasi proses penyerangan hingga selesai, anda dapat mengunduh **Ransomware Sample_Complete Attack Simulation(Password 111111).zip** di PMO

 Ransomware Sample_Complete Attack Simulation(Password 111111).

Name	Size	Packed	Type	Modified	CRC32
Local Disk					
\1.js *	1,435	646	JavaScript File	7/4/2019 3:57 PM	999D6CFD
\1.bat *	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 9:08 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
\cygcc_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
\cygiconv-2.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
\cymysqlclient-18.dll *	2,887,197	736,200	Application extension	7/4/2019 3:57 PM	21F40235
\cypcre-1.dll *	282,151	92,512	Application extension	7/4/2019 3:57 PM	202A26C
\cypcq-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	2F0E0A3FC
\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	214D6680
\libgcc_s_dw2-1.dll *	112,654	47,902	Application extension	7/4/2019 3:57 PM	72DC885E
\libssh.dll *	382,659	144,794	Application extension	7/4/2019 3:57 PM	1A0AED2
\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, virus awalnya akan menyerang PC 2 di LAN yang sama melalui via RDP brute-force attack. Setelah proses penyerangan selesai, file pada PC 1, dan juga file pada PC 2 telah terenkripsi.

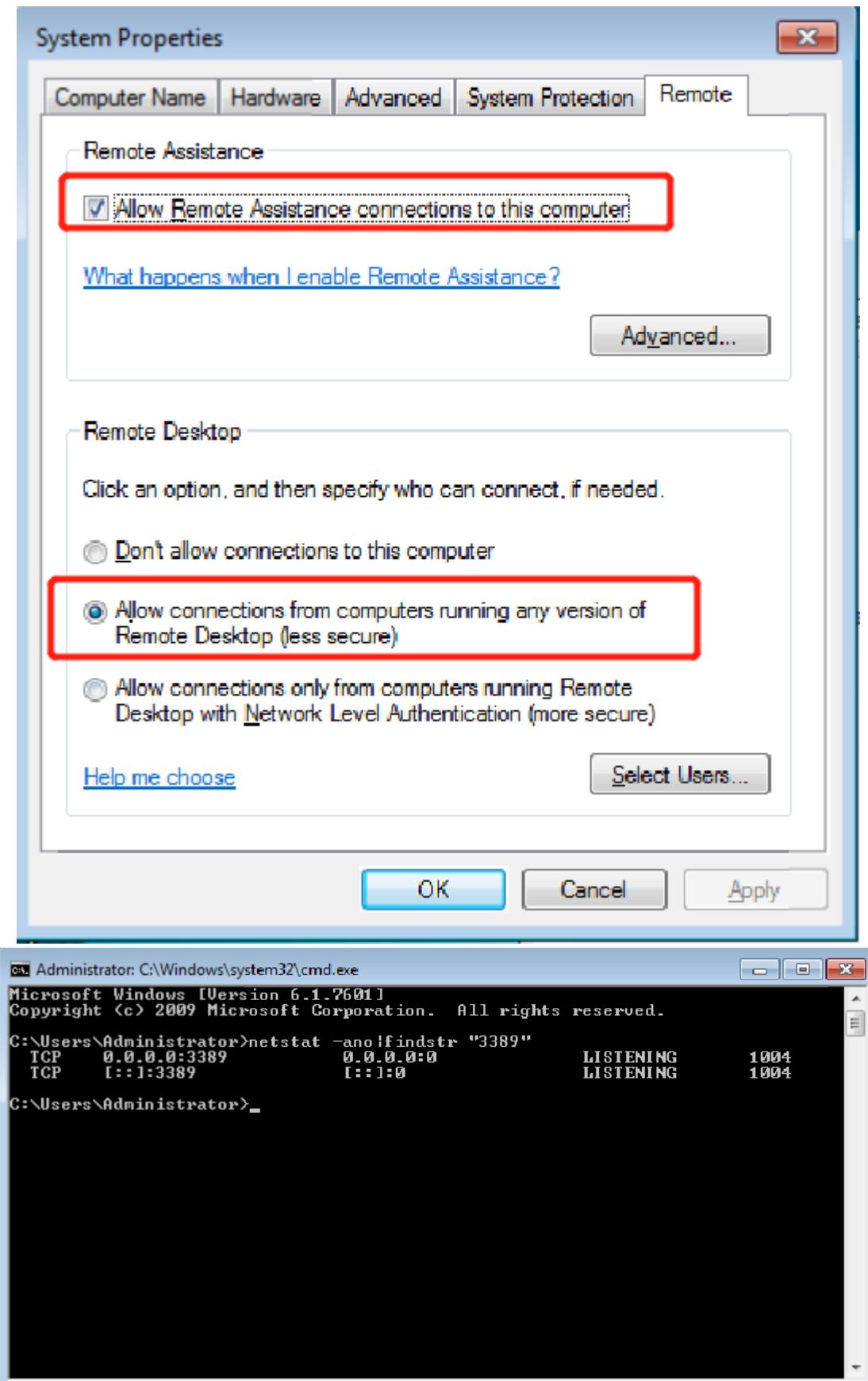
2.3 Konten

Tahap	Konten	Hasil yang Diharapkan
Ronde 4	Pada Endpoint Secure MGR, aktifkan policy perlindungan untuk enable the protection policy PC 1 dan PC 2 (mengaktifkan perlindungan	1. PC 1 dan PC 2 telah terlindungi oleh policy anti-ransomware policy pada Endpoint Secure, dimana

	pemancingan ransomware), dan demonstrasi proses penyerangan dan efek dari ransomware.	memblok operasi ransomware. Sebagai hasil, file pada kedua PC 1 dan PC 2, tidak terenkripsi oleh ransomware.
--	---	--

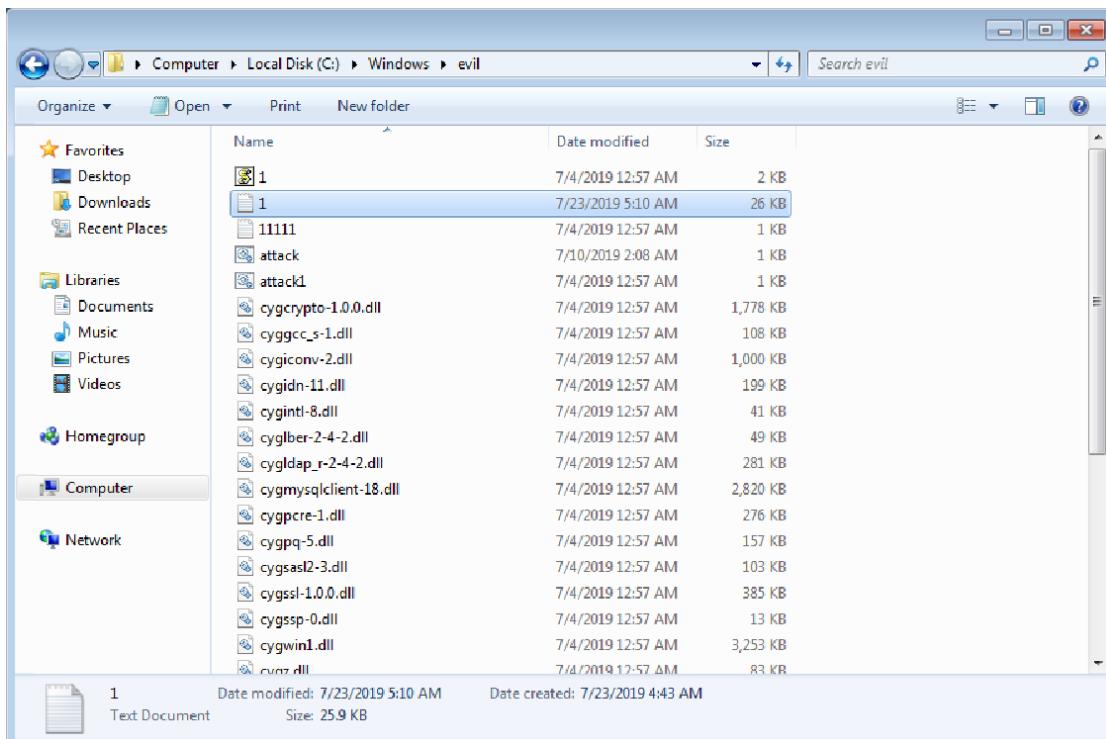
2.4 Deskripsi

- (1) Demonstrasi ini hanya dapat diterapkan kepada kondisi lingkungan virtual yang di deploy di client maupun pc persoanl, dan demonstrasi harus disolasi dari network bisnis pelanggan, sehingga menghindari ransomware mengenkripsi komputer lainnya.
- (2) Anda dapat melakukan pengaturan pada MGR, PC 1, dan PC 2 sendiri. PC 1 dan PC 2 butuh diinstal Endpoint Secure Agent.
- (3) Biasanya, PC 1 dan PC 2 berjalan di Windows 7 SP1.
- (4) PC 1 dan PC 2 dapat menggunakan alamat dari segment network 20.10.0.0/24. Program ransomware akan secara otomatis memindai PC lain yang berada pada segmen network yang sama.
- (5) Anda disarankan mematikan system firewall windows anda dan mengaktifkan service RDP di PC dimana ransomware akan menyerang melalui port 3389 di PC 2.

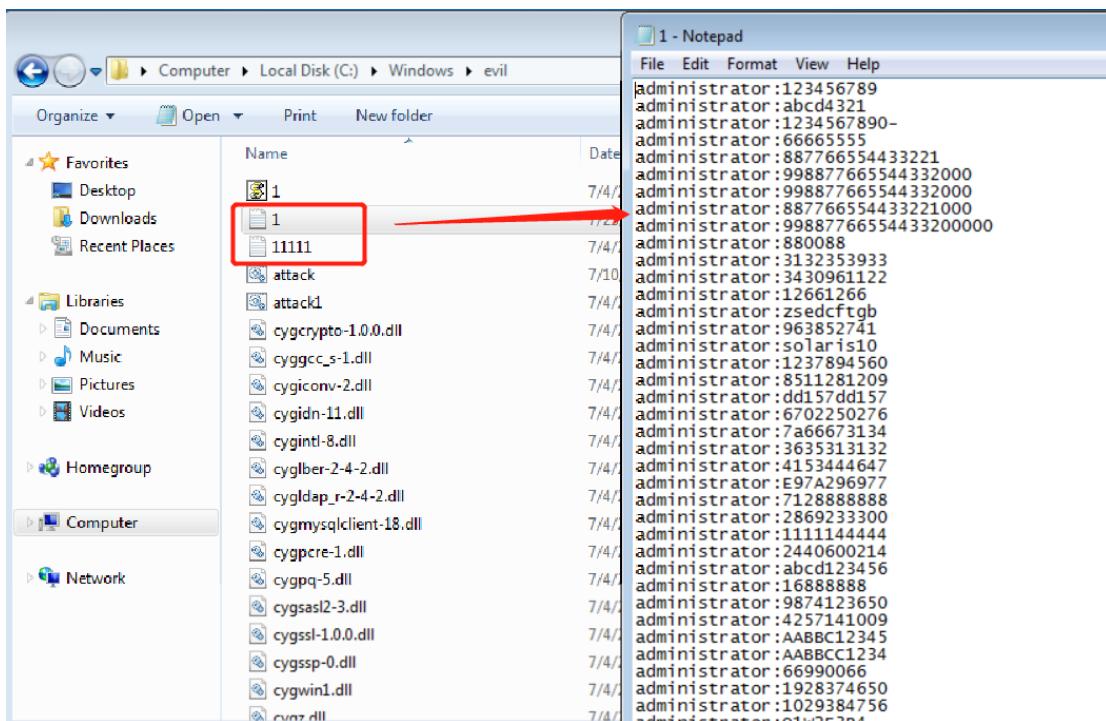


(6) Contoh ransomware butuh ditempatkan di direktori yang spesifik.

Use Honeypot to Anti Ransomware



(7) Password digunakan untuk penyerangan virus normalnya ditempatkan pada file text. Kemudian, ketika anda menggunakan system windows 7 anda, pastikan password yang digunakan terdapat dalam text file (mengandung password normal).pada perlengkapan virus.Sangat direkomendasikan untuk menggunakan administrator/11111 sebagai username dan password.



2.5 Resiko

Item Resiko	Deskripsi
Pengisolasian lingkungan demonstrasi	Sejak ransomware dijalankan, demonstrasi akan dijalankan di lingkungan virtual dan harus diisolasi dari network yang sesungguhnya. Jika gagal dilakukan file pada komputer lain akan diserang oleh ransomware.
Snapshot PC yang digunakan untuk demonstrasi	Selama demonstrasi. File di PC akan terenkripsi. Untuk mengembalikannya secara cepat untuk demonstrasi selanjutnya, anda membutuhkan melakukan snapshot lebih dahulu.

Bagian 3 Proses Demonstrasi

3.1 Alur

3.1.1 Konten

Pada Endpoint Secure Agent, aktifkan protection policy untuk PC 1 dan PC 2 (mengaktifkan umpan pelindungan ransomware), dan mendemonstrasikan proses penyerangan dan efek dari ransomware..

3.1.2 Hasil yang diharapkan

PC 1 dan PC 2 akan terlindungi oleh ransomware bait policy dari Endpoint Secure, dimana akan memblok operasi ransomware. Sebagai hasilnya, file di kedua PC 1 dan PC 2, tidak terenkripsi oleh ransomware.

3.1.3 Langkah Langkah

3.1.3.1 Mengembalikan dari Snapshots

- (1) Roll back PC 1, PC 2, dan MGR ke snapshots yang sebelumnya.
- (2) Periksa MGR dan temukan apakah kedua PC 1 dan PC 2 sudah online, seperti ditunjukkan dibawah:

Use Honeypot to Anti Ransomware

The screenshot shows the Sangfor Endpoint Secure interface. The top navigation bar includes Home, Endpoints, Micro-Segmentation, Detection, Response, Logs, and System. The Endpoints tab is selected, showing a list of endpoints. On the left sidebar, under Groups, there is a section for Endpoints, which is currently expanded, showing a Local Site and Ungrouped En... (with a red box around it). The main panel displays 'Endpoints (2 online / 2 in total)' with two entries: Windows1 (IP 20.10.0.3) and Windows2 (IP 20.10.0.8), both marked as Online.

3.1.3.2 Pengaturan Policy

Mengaktifkan ransomware protection policy pada PC 1 dan PC 2. Pilih **Endpoints > Security Protection**. Atur **Ungrouped Endpoints** policy (Kedua PC 1 dan PC 2 menjadi online pada get ungrouped endpoints secara default) dan lanjutkan ke tab **Realtime Protection**. Aktifkan **Ransomware Protection** dan **Realtime File System Protection** policies. **Hidupkan semua icon yang terkunci** seperti yang ditunjukkan di bawah (pada kotak merah)

The screenshot shows the Sangfor Endpoint Secure interface with the Security Protection tab selected. In the center, under the Realtime Protection tab, the Realtime File System Protection section is highlighted with a red box. It contains the following configuration:

- Enable realtime file system protection:** A checked checkbox.
- Protection Level:** Medium (radio button selected).
- File Type:** Document, Script, Executable file (checkboxes selected).
- Scan Options:** Skip files larger than 50 MB, Scan compressed files up to 3 layers deep.
- Engine:** Sangfor Engine Zero, Gene Analytic Engine (checkboxes selected).
- Action:** Standard (radio button selected).

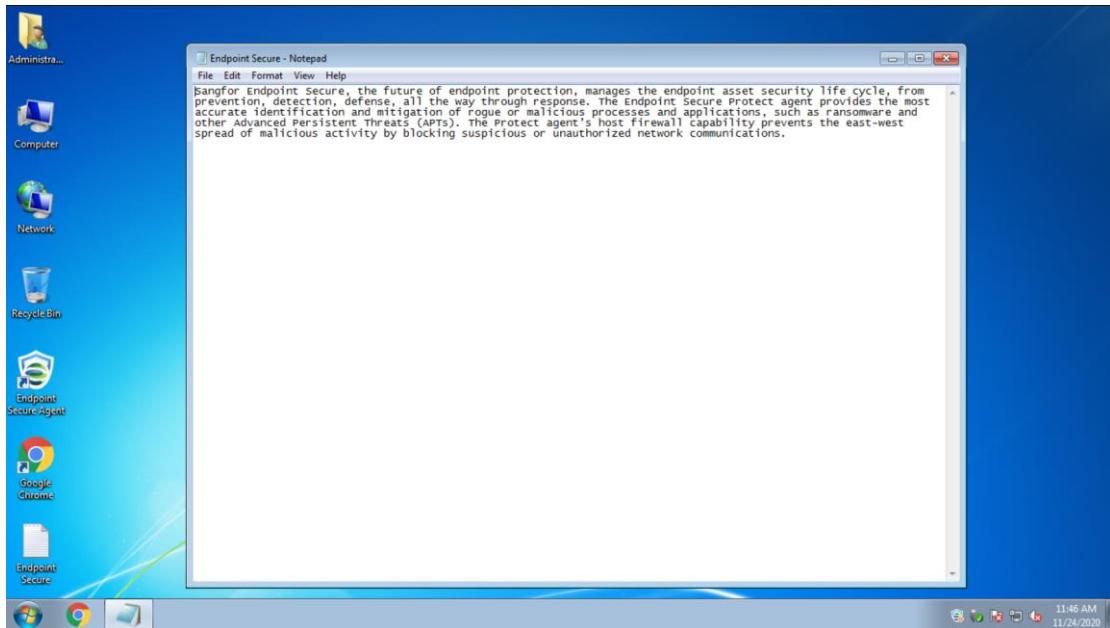
Use Honeypot to Anti Ransomware

The screenshot shows the Sangfor Endpoint Secure interface under the 'Endpoints' tab. In the left sidebar, 'Security Protection' is selected. On the right, the 'Ransomware Protection' section is highlighted with a red box. It contains the following configuration:

- Type: Realtime (checkbox checked)
- Scheduled: Every day, 00:00:00
- Action: Fix (radio button selected)
- Enable ransomware honeypot (checkbox checked)
- Action: Fix (radio button selected)

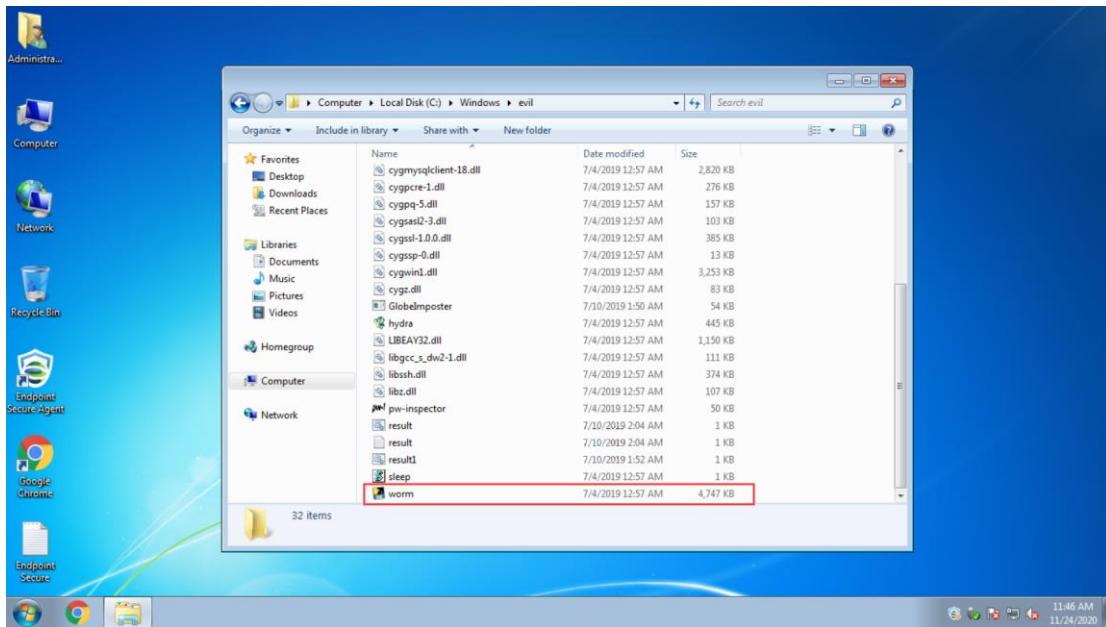
3.1.3.3 Menginisiasi Penyerangan

(1) Sebelum menginisiasi penyerangan, periksa status dari PC 1 dan PC 2, file pada kedua komputer tidak terenkripsi dan dapat dibuka dengan normal, seperti pada tampilan dibawah:



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

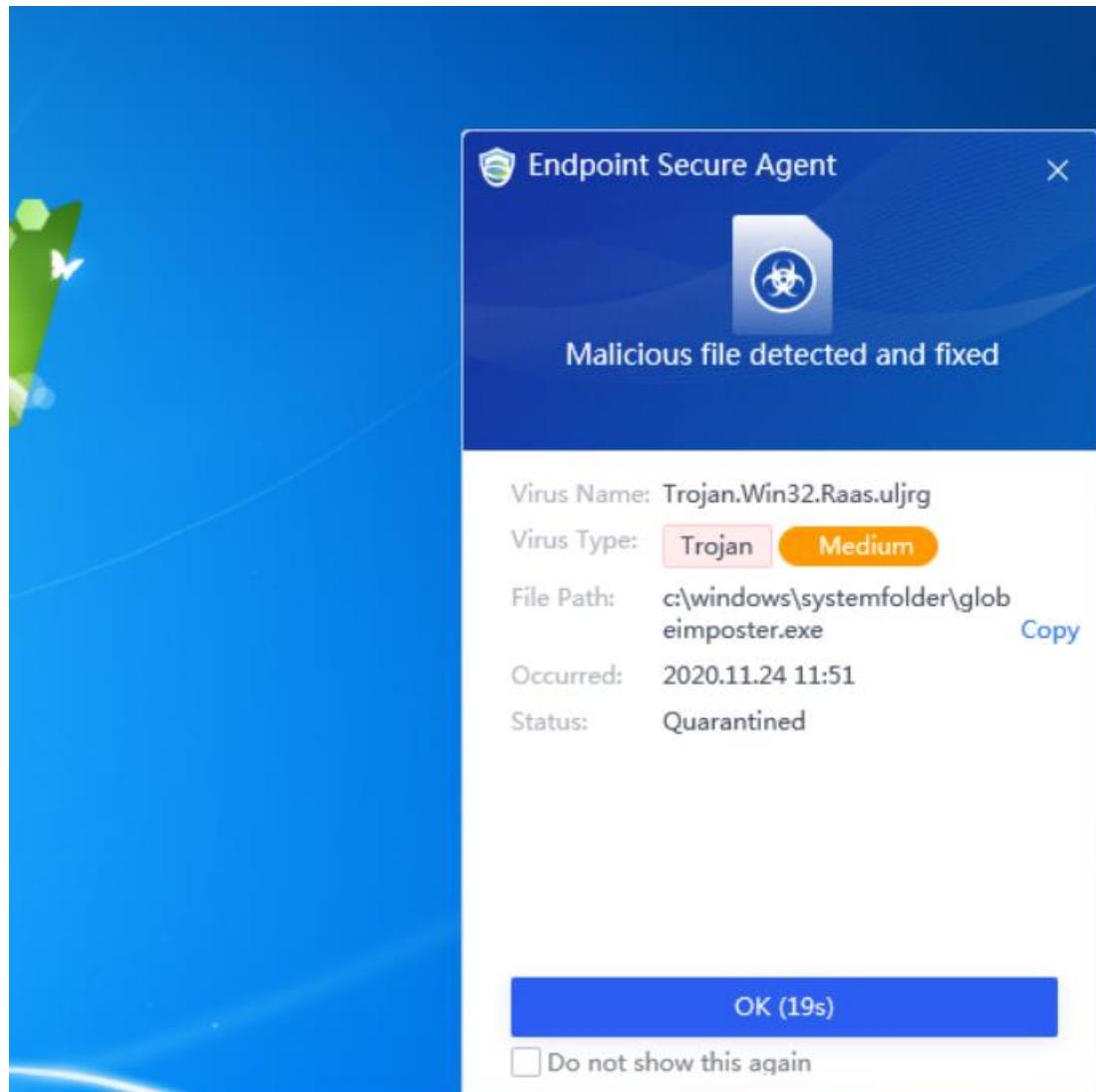
Use Honeypot to Anti Ransomware



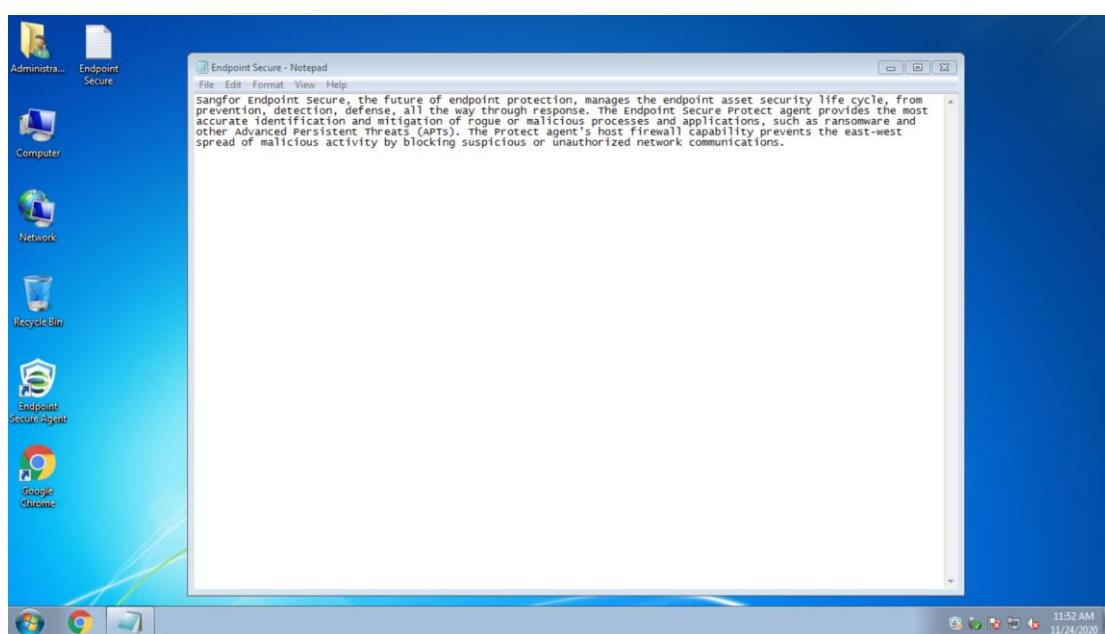
3.1.3.4 Efek Penyerangan

Karena PC 1 dan PC 2 telah terlindungi oleh ransomware protection policy dari Endpoint Secure, ketika ransomware terdeteksi, sistem secara otomatis mengkarantina ransomware dan menampilkan halaman peringatan Hal ini melindungi PC 1 dan PC 2 terhadap enkripsi ransomware.

Use Honeypot to Anti Ransomware

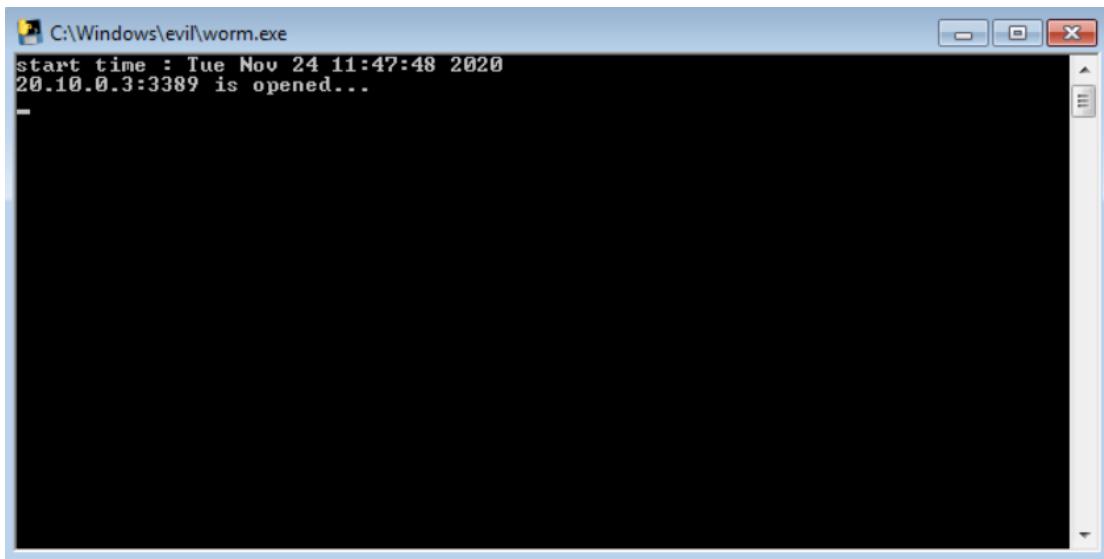


Tampilan file pada PC 1 dan PC 2. Mereka tidak terenkripsi, seperti tampilan dibawah:



Bagian 4 Anjuran

1. Ketika program virus berjalan, sistem akan berhenti merespon beberapa kali dan tidak bereaksi pada posisi yang sama sekitar 2 menit. Pada kasus ini, anda bisa menutup dan merestart program.





Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc