DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PEDOMAN PENANGANAN INSIDEN

MALICIOUS SOFTWARE (MALWARE)

Dinas Komunikasi dan Informatika Kota Batam

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PENDAHULUAN

Malware, atau Malicious Software, merupakan suatu definisi yang diberikan untuk setiap program atau file atau kode yang dapat membahayakan suatu sistem. Malware berusaha menyerang, merusak, atau menonaktifkan komputer, sistem komputer, jaringan, tablet, dan perangkat seluler, sering kali dengan mengambil sebagian kendali atas operasi perangkat.

Malware modern saat ini kebanyakan bukan bertujuan untuk merusak, namun lebih ke arah pencurian data sensitif. Adapun malware yang menyebabkan kerusakan dan kehilangan data biasanya berupa ransomware, yang mengancam user yang menjadi korban untuk membayar sejumlah tebusan jika tidak ingin datanya hilang

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

TUJUAN

1. Memastikan adanya sumber daya yang memadai untuk menangani serangan yang terjadi
2. Melakukan pengumpulan informasi yang akurat
3. Meminimalisir dampak dari insiden yang terjadi
4. Mencegah adanya insiden lanjutan dan mencegah kerusakan agar tidak lebih meluas

RUANG LINGKUP

Panduan ini berisi langkah-langkah yang harus diambil apabila terjadi insiden malware, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan insiden

Panduan ini dapat dijadikan acuan bagi semua individual atau tim (administrator, pengelola TI, dan tim respon insiden keamanan siber) yang bertanggung jawab untuk mencegah, mempersiapkan, atau menanggapi insiden malware

PROSEDUR PENANGANAN INSIDEN MALWARE

Penanganan terhadap insiden malware dapat dilakukan dalam beberapa tahap seperti pada gambar berikut

DISKOMINFO BATAM

PERSIAPAN

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

1. Pembentukan Tim Respon, tim dapat berasal dari internal organisasi/institusi atau jika memang diperlukan dapat berasal dari luar organisasi/institusi (eksternal). Anggota tim memiliki pengetahuan tentang malware dan memiliki kemampuan penanganan insiden malware

2. Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden. Dokumen ini antara lain adalah :
   - Panduan Penanganan Insiden Siber
   - Formulir Penanganan Insiden Siber
   - Dokumen Kebijakan, diantaranya kebijakan keamanan, kebijakan pengunaan laptop, antivirus, internet dan email, serta kebijakan backup
   - Dokumen Baseline Performance
   - Dokumen Audit Sistem
   - Dokumen Profil dari semua perangkat lunak dan proses-proses yang harus berjalan pada sistem berdasarkan proses bisnis organisasi
   - Database penanganan insiden yang pernah terjadi sebelumnya
   - Daftar yang memuat indikasi-indikasi suatu komputer atau jaringan terkena malware, misalkan daftar aplikasi yang telah terindikasi terkena malware, alamat IP terkait dengan Command and Control (C&C)

3. Menentukan tempat (ruangan) untuk penanganan

4. Menentukan lingkungan yang aman untuk analisa malware agar dampak malware tidak menyebar ke sistem yang lain.

PERSIAPAN

Menyiapkan tools yang akan digunakan, diantaranya:

- Tools untuk penyaringan misalnya, Squid merupakan perangkat lunak open source pada web proxy yang mendukung filter URL
- Tools untuk menghitung nilai hash
- Tools untuk deteksi virus baik berbasis host maupun onlinemisalnya antivirus dan website www.virustotal.com
- Tools pendeteksi berbasis host, misalnya Samhain, OSSEC dan Osiris
- Tools untuk analisa malware, meliputi Mesin uji, merupakan mesin virtual untuk melakukan analisis terhadap malware. Utility toolkit, tools ini digunakan untuk mengumpulkan sampel untuk analisis malware atau untuk mengidentifikasi, menampung, dan memberantas malware, misalnya SysInternals. Reverse Engineering tools, merupakan tools yang digunakan untuk melakukan analisa lebih lanjut terkait source code dari sampel malware

IDENTIFIKASI DAN ANALISIS

PROSES

1. Memeriksa apakah antivirus berfungsi normal atau tidak
2. Mengecek file yang tidak dikenal pada root atau system directory
3. Memeriksa file dengan ekstensi ganda. Sangat disarankan untuk menonaktifkan opsi fitur 'sembunyikan ekstensi' pada file explorer untuk mengetahui ekstensi yang sebenarnya dari suatu file
4. Memeriksa proses dan service yang tidak dikenal dalam sistem menggunakan Task Manager
5. Memeriksa utilitas sistem, misalnya Task Manager atau SysInternals Process Explorer
6. Memeriksa penggunaan memory CPU menggunakan Task Manager
7. Memeriksa anomali pada Registry Key

IDENTIFIKASI DAN ANALISIS

PROSES

8. Memeriksa anomali pada traffic jaringan. Malware modern saat ini kebanyakan memiliki fitur “Command and Control” dimana biasanya setiap malware yang sudah menginfeksi suatu sistem, akan mengirimkan sinyal kepada induk malware melalui aktivitas “Command and Control” tersebut

9. Identifikasi anomali proses dan service yang dibuat pada Task Scheduler

10. Identifikasi user account pada sistem. Beberapa malware mempunyai kemampuan untuk membuat user account baru pada sistem operasi yang terinfeksi.

11. Identifikasi entry log pada sistem operasi menggunakan Event Viewer

12. Identifikasi proses yang mencurigakan menggunakan SysInternals Tools

CONTAINMENT

01 Meminta izin kepada pemilik sistem untuk memutus sistem yang terinfeksi malware dari jaringan

02 Isolasi sistem yang terinfeksi malware. Hal ini dapat dilakukan dengan cara mencabut kabel LAN atau memindahkan sistem tersebut ke VLAN khusus

03 Mengubah konfigurasi routing table pada Firewall untuk memisahkan sistem yang terinfeksi malware dengan sistem lainnya

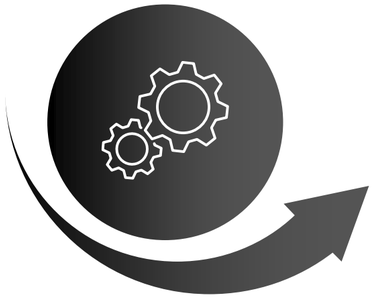
04 Melakukan backup data pada sistem yang terinfeksi malware

05 Identifikasi gejala kemiripan pada sistem lain untuk mencegah penyebaran malware. Jika terdapat kemiripan, maka sistem tersebut juga harus dilakukan proses containment

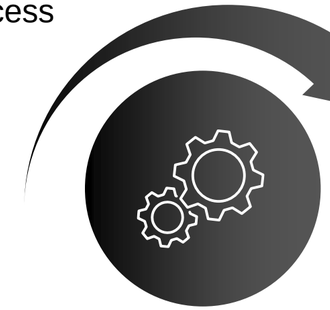
ERADICATION

1 Menghentikan proses yang terindikasi sebagai proses yang malicious, dengan cara sebagai berikut

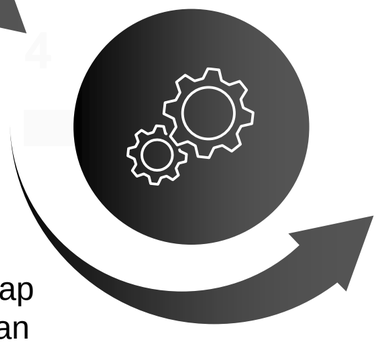
Tidak melakukan kill / end process terhadap malicious process tersebut, dikarenakan malware akan melakukan autostart process ketika prosesnya terhenti



Lakukan suspend terhadap proses tersebut, kemudian lakukan record pada path EXE proses tersebut dan file DLL yang dipanggil oleh proses tersebut



Dalam kondisi sleep (proses di suspend), kemudian satu persatu lakukan kill process dari kumpulan malicious process tersebut dimulai dari child process ke parent process



Jika malicious process masih melakukan autostart atau mengganti namanya dengan nama proses baru, maka perlu didokumentasikan lebih lanjut dan simpan malicious program tersebut ke media lain untuk proses analisa yang lebih mendetail

DISKOMINFO BATAM

ERADICATION

2 Menghapus autostart process yang mencurigakan dari hasil analisa aplikasi autostart:

3 Jika proses tersebut kembali lagi, jalankan Process Monitor untuk mengidentifikasi apakah ada lokasi lain dimana malware tersebut bersembunyi

4 Lakukan proses di atas secara berulang hingga dapat dipastikan semua malicious program telah dihapus dan prosesnya sudah di kill process

5 Setelah program malware dihapus dan malicious process di kill process, lakukan full scanning terhadap sistem menggunakan signature antivirus yang sudah diperbaharui.

G20 INDONESIA 2022 BerAKHLAK

ERADICATION

6 Jika proses scanning antivirus tidak dapat dilakukan karena telah diblokir oleh malware, lakukan proses sebagai berikut

Booting sistem melalui Live usb rescue disk, misalnya Hiren Boot CD, Kaspersky Rescue Disk, dll

Live usb tersebut dapat berupa sistem operasi Linux ataupun miniXP yang berisi beberapa tools. Lakukan proses mounting sistem operasi yang terinfeksi ke dalam Live usb yang sedang berjalan

Lakukan proses scanning antivirus dan antimalware pada Live usb yangsedang berjalan

7 Jika terdapat user-user yang dibuat oleh malware, maka hapus user-user yang tidak dikenali tersebut untuk menghindari masuknya kembali malware melalui user yang tidak dikenal tersebut

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaborasi

PEMULIHAN

LANGKAH-LANGKAH

1. Validasi sistem untuk memastikan sudah tidak ada aplikasi atau file yang rusak atau terinfeksi malware.

2. Melakukan aktivitas monitoring untuk memastikan apakah malware masih ada atau kembali lagi setelah proses eradication dengan melakukan hal-hal sebagai berikut :

   i. Memantau proses dan servis yang berjalan menggunakan Process Monitor dan Process Explorer

   ii. Memantau aktivitas traffic jaringan menggunakan tools wireshark atau tcpdump untuk memantau apakah ada request outgoing atau traffic incoming yang mencurigakan

3. Jika terjadi kerusakan yang cukup parah (file sistem terhapus, data penting hilang, menyebabkan kegagalan booting pada sistem operasi), maka sistem dibangun ulang dari file backup terakhir sistem yang dimiliki

4. Melakukan patching sistem

5. Melakukan hardening terhadap sistem

6. Menambahkan signature dari malware ke sistem monitoring atau database antivirus

TINDAK LANJUT

Membuat dokumentasi dan laporan terkait penanganan insiden malware, yang berisi langkah-langkah dan hasil yang telah didapatkan

Memberikan analisa dan penjelasan apa yang harus dilakukan, sehingga meminimalisir insiden serupa tidak terulang kembali.

Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya

Membuat evaluasi dan rekomendasi. Rekomendasi seperti Penambahan pengetahuan tentang penanganan insiden malware, misalnya melalui pelatihan

Mendokumentasikan malware terkait jalan masuk, perilaku, dampak kerusakan yang terkait malware ke dalam database malware

Menyempurnakan langkah-langkah respon atau prosedur penanganan insiden malware yang ada

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PEDOMAN PENANGANAN INSIDEN

MALICIOUS SOFTWARE (MALWARE)

Dinas Komunikasi dan Informatika Kota Batam