PANDUAN PENANGANAN INSIDEN
MALICIOUS SOFTWARE (MALWARE)

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI BALI

Versi Dokumen

No	Tanggal	Versi Dokumen	Oleh	Keterangan
1	Desember 2021	Versi 1.0	Diskominfos Prov. Bali	-

Kata Pengantar

Puji syukur kehadirat Tuhan Yang Maha Esa, atas segala limpahan rahmat, nikmat serta karunia-Nya yang tak ternilai dan tak dapat dihitung sehingga kami dapat menyelesaikan penyusunan “Panduan Penanganan Insiden *Malicious Software* (*Malware*)”. Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam pelaporan insiden siber. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi insiden siber, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Panduan ini tentu saja masih banyak kekurangan dan masih jauh dari kesempurnaan karena keterbatasan ilmu dan referensi kami. Untuk itu, kami selalu berusaha melakukan evaluasi dan perbaikan secara berkala agar bisa mencapai hasil yang lebih baik lagi.

Akhir kata, kami ucapkan terima kasih kepada segala pihak yang telah membantu dalam penyusunan panduan ini.

Bali, 2 Desember 2021

Ditandatangani secara elektronik oleh :
KEPALA DINAS
Gede Pramana
NIP. 19680531 199703 1 002

Daftar Isi

Prosedur Penanganan *Malicious Software* (*Malware*)

1. 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* menjadi salah satu ancaman yang paling besar dalam insiden keamanan informasi. Berdasarkan riset dari *Verizon Data Breach Investiogation Report* 2017, aktivitas insiden yang melibatkan *malware* menduduki peringkat kedua. Pada riset tersebut juga menyebutkan bahwa aktivitas insiden *malware* menyebabkan kehilangan data dan kerugian finansial yang cukup signifikan. *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.

2. TUJUAN

Secara umum, tujuan panduan ini dimaksudkan untuk membantu organisasi memahami tentang penanganan suatu insiden yang disebabkan oleh *malware*. Penanganan insiden *malware* yang dilakukan dengan tepat dan cepat, akan sangat bermanfaat untuk mengurangi resiko yang diakibatkan oleh *malware* tersebut. Sedangkan secara khusus adalah sebagai berikut:

a. Memastikan adanya sumber daya yang memadai untuk menangani insiden yang terjadi;
b. Melakukan pengumpulan informasi yang akurat;
c. Meminimalisir dampak dari insiden;
d. Mencegah adanya insiden lanjutan dan mencegah kerusakan agar tidak lebih meluas.

3. 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*.

4. PROSEDUR PENANGANAN INSIDEN *MALWARE*

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

Gambar 1. Tahap Penanganan Insiden *Malware*

4.1. Persiapan

Tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang, dimana akan digunakan pada proses penanganan terhadap insiden. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden, merupakan persiapan yang mendasar bagi penanganan insiden yang disebabkan oleh *malware*.

a) 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*.

b) Penyiapan Dokumen Legal

Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden *malware*. Dokumen ini antara lain:

- Panduan Penanganan Insiden Siber.
- Formulir Penanganan Insiden Siber.
- Dokumen Kebijakan, diantaranya kebijakan keamanan, kebijakan penggunaan 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).

c) Menentukan tempat (ruangan) untuk penanganan.
d) Menentukan lingkungan yang aman untuk analisa *malware* agar dampak *malware* tidak menyebar ke sistem yang lain.
e) Menyiapkan *tools* yang akan digunakan, diantaranya:
   - *Tools* untuk penyaringan, misalnya:
     a. *Squid* merupakan perangkat lunak *open source* pada web *proxy* yang mendukung filter URL;
     b. *Squid Guard* adalah *tools* yang dapat digunakan untuk menyederhanakan tugas filter URL yang merupakan *plug-in* untuk *squid* yang merupakan kombinasi dari filter, *redirector*, dan akses kontrol, yang dapat digunakan untuk membuat aturan akses berdasarkan pada waktu, kelompok pengguna, dan URL.
   - *Tools* untuk menghitung nilai *hash*.
   - *Tools* untuk deteksi virus baik berbasis *host* maupun *online*, misalnya antivirus dan *website* www.virustotal.com
   - *Tools* pendeteksi berbasis *host*, misalnya *Samhain*, *OSSEC* dan *Osiris*.
   - *Tools* untuk analisa *malware*, meliputi :
     a. Mesin uji, merupakan mesin virtual untuk melakukan analisis terhadap *malware*, misalnya *VMWare*, *MS VPC*, dan *Xen*. Mesin uji ini diperlukan dalam melakukan analisa *malware* menggunakan metode analisa dinamis.
     b. *Utility toolkit*, *tools* ini digunakan untuk mengumpulkan sampel untuk analisis *malware* atau untuk mengidentifikasi, menampung, dan memberantas *malware*, misalnya *SysInternals*.
     c. *Reverse Engineering tools*, merupakan *tools* yang digunakan untuk melakukan analisa lebih lanjut terkait *source code* dari sampel *malware*, misalnya *IDA-Pro*, *CFF Explorer*, dan *WinHex*. *Reverse Engineering tools* diperlukan dalam melakukan analisa *malware* menggunakan metode analisa statis.

4.2. Identifikasi dan Analisis

Tahap ini merupakan tahap identifikasi adanya *malware*. Proses-proses yang dilakukan dalam tahap identifikasi adalah sebagai berikut :

a. Memeriksa apakah antivirus berfungsi normal atau tidak. Hal ini karena ada *malware* yang dapat menghancurkan instalasi antivirus dengan merusak *executable file*, mengubah kunci registri atau merusak file definisi, maupun menonaktifkan *update* dari *signature* suatu file.

b. Mengecek file yang tidak dikenal pada *root* atau *system directory*.

c. Memeriksa file dengan ekstensi ganda. Sangat disarankan untuk menonaktifkan opsi fitur 'sembunyikan ekstensi' pada *file explorer* untuk mengetahui ekstensi yang sebenarnya dari suatu file.

d. Memeriksa proses dan *service* yang tidak dikenal dalam sistem menggunakan *Task Manager*

e. Memeriksa utilitas sistem, misalnya *Task Manager* atau *SysInternals Process Explorer*. Terdapat *malware* yang menonaktifkan utilitas ini sehingga tidak dapat dijalankan.

f. Memeriksa penggunaan *memory* CPU menggunakan *Task Manager*.

g. Memeriksa anomali pada *Registry Key*.

h. 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.

i. Identifikasi anomali proses dan *service* yang dibuat pada *Task Scheduler*.

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

k. Identifikasi *entry log* pada sistem operasi menggunakan *Event Viewer*.

l. Identifikasi proses yang mencurigakan menggunakan *SysInternals Tools*. *SysInternal Tools* merupakan salah satu kumpulan *tools* utilitas milik *Microsoft* yang bertujuan untuk mengidentifikasi sistem lebih

mendetail. Beberapa Aplikasi *SysInternal tools* yang paling banyak digunakan untuk melakukan identifikasi dan analisa *malware* adalah *Process Explorer*, *Autoruns*, dan *Process Monitor*.

4.3. *Containment*

Tahap ini bertujuan untuk menghentikan atau mencegah penyebaran *malware*. Prosedur yang dilakukan pada tahap *containment* adalah sebagai berikut :

a. Meminta izin kepada pemilik sistem untuk memutus sistem yang terinfeksi *malware* dari jaringan.
b. Isolasi sistem yang terinfeksi *malware*. Hal ini dapat dilakukan dengan cara mencabut kabel LAN atau memindahkan sistem tersebut ke VLAN khusus. Namun, perlu menyimpan informasi koneksi jaringan pada sistem sebelum memutuskan hubungan dari jaringan yang mungkin akan dibutuhkan dalam melakukan analisa selanjutnya.
c. Mengubah konfigurasi *routing table* pada *Firewall* untuk memisahkan sistem yang terinfeksi *malware* dengan sistem lainnya.
d. Melakukan *backup* data pada sistem yang terinfeksi *malware*.
e. Identifikasi gejala kemiripan pada sistem lain untuk mencegah penyebaran *malware*. Jika terdapat kemiripan, maka sistem tersebut juga harus dilakukan proses *containment*.

4.4. *Eradication*

Tahap ini merupakan tahapan dimana beberapa teknik yang berbeda-beda digunakan untuk melakukan analisa terhadap *malware* dan menghapus *malware* dari sistem yang telah terinfeksi. Setelah file yang terinfeksi diidentifikasi, gejala *malware* dicatat dan *executable malware* diidentifikasi dan dianalisis, kemudian semua file *executables malware* dan artefak yang ditinggalkan oleh *malware* akan dihapus, serta menutup *port* yang terindikasi sebagai lubang masuknya *malware*. Proses-proses yang dilakukan dalam tahap ini adalah sebagai berikut :

a. Menghentikan proses yang terindikasi sebagai proses yang *malicious*, dengan cara sebagai berikut :
   i. Tidak melakukan *kill/end process* terhadap *malicious process* tersebut. Hal ini dikarenakan *malware* akan melakukan *autostart process* ketika prosesnya terhenti.
   ii. Lakukan *suspend* terhadap proses tersebut, kemudian lakukan *record* pada *path* EXE proses tersebut dan file DLL yang dipanggil oleh proses tersebut.

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

b. Menghapus *autostart process* yang mencurigakan dari hasil analisa aplikasi *autostart*.
c. Jika proses tersebut kembali lagi, jalankan *Process Monitor* untuk mengidentifikasi apakah ada lokasi lain dimana *malware* tersebut bersembunyi.
d. Lakukan proses di atas secara berulang hingga dapat dipastikan semua *malicious* program telah dihapus dan prosesnya sudah di *kill process*.
e. Setelah program *malware* dihapus dan *malicious process* di *kill process*, lakukan *full scanning* terhadap sistem menggunakan *signature* antivirus yang sudah diperbaharui.
f. Jika proses *scanning* antivirus tidak dapat dilakukan karena telah diblokir oleh *malware*, maka lakukan proses sebagai berikut :
   i. *Booting* sistem melalui *Live usb rescue disk*, misalnya *Hiren Boot* CD, *FalconFour's Ultimate Boot* CD, *Kaspersky Rescue Disk*, dll.
   ii. *Live usb* tersebut dapat berupa sistem operasi *Linux* ataupun *miniXP* yang berisi beberapa *tools* seperti *defragment tools*, *driver tools*, *backup* dan *recover data tools*, antivirus dan anti-*malware tools*, *rootkit detection tools*, *secure data wiping tools*, *partitioning tools*, *password recovery tools*, *network tools*, *recover/repair broken partitions tools*, dll. Lakukan proses *mounting* sistem operasi yang terinfeksi ke dalam *Live usb* yang sedang berjalan.
   iii. Lakukan proses *scanning* antivirus dan anti-*malware* pada *Live usb* yang sedang berjalan
g. 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.

4.5. Pemulihan

Pemulihan merupakan tahap untuk memulihkan data sistem yang terinfeksi *malware* serta mengembalikan seluruh sistem agar bekerja normal seperti semula. Langkah yang dilakukan terhadap pemulihan sistem, diantaranya:

a. Validasi sistem untuk memastikan sudah tidak ada aplikasi atau file yang rusak atau terinfeksi *malware*. Begitu pula kesalahan atau kekurangan konfigurasi sistem untuk kemudian disesuaikan kembali.

b. Melakukan aktivitas *monitoring* untuk memastikan apakah *malware* masih ada atau kembali lagi setelah proses *eradication* dengan malakukan 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, serta *request query* DNS karena *malware* yang memiliki kemampuan *Command and Control* biasanya melakukan kontak dengan induknya.
c. 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.
d. Melakukan *patching* sistem.
e. Melakukan *hardening* terhadap sistem.
f. Menambahkan *signature* dari *malware* ke sistem *monitoring* atau *database* antivirus.

4.6. Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk masa mendatang. Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Membuat dokumentasi dan laporan terkait penanganan insiden *malware*, yang berisi langkah-langkah dan hasil yang telah didapatkan.
b. Memberikan analisa dan penjelasan apa yang harus dilakukan, sehingga meminimalisir insiden serupa tidak terulang kembali.
c. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.
d. Membuat evaluasi dan rekomendasi. Rekomendasi yang dapat diberikan diantaranya:
   - Penambahan pengetahuan tentang penanganan insiden *malware*, misalnya melalui pelatihan.
   - Memperbaharui anti *malware* dengan *signature* file yang baru, dengan harapan dapat berhasil dalam mendeteksi dan menghapus *malware.*
   - Meningkatkan pertahanan sistem terhadap *malware.*
a. Mendokumentasikan *malware* terkait jalan masuk, perilaku, dampak kerusakan dan lain-lain yang terkait *malware* ke dalam *database malware*.
b. Menyempurnakan langkah-langkah respon atau prosedur penanganan insiden *malware* yang ada.