Government Computer Security Incident Response Team

BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI

PANDUAN

PENANGANAN INSIDEN

MALWARE

Diadopsi dari : SOP Incident Handling Malware
Kementrian Komunikasi dan Informastika Republik Indonesia

BPPT CSIRT
2014

DAFTAR ISI

BAGIAN 1 : PENDAHULUAN

Suatu insiden yang disebabkan oleh malware. Petunjuk Teknis ini untuk memberikan arahan pelaksanaan kerja yang berhubungan dalam bidang Teknologi Informasi, khusus untuk menagani permasalahan Malware. Malware adalah perangkat lunak berbahaya, perangkat lunak ini bisa digunakan untuk mengganggu pengoperasian komputer, mengumpulkan informasi sensitif, atau mendapatkan akses ke sistem komputer. Bentuk Malware ini dapat muncul dalam bentuk kode dieksekusi (exe), script, konten aktif, dan perangkat lunak lainnya. 'Malware' adalah istilah umum yang digunakan untuk merujuk kepada berbagai bentuk perangkat lunak yang bersikap bermusuhan atau mengganggu.

Malware termasuk virus komputer, worm, trojan horse, ransomware, spyware, adware, scareware, dan program berbahaya lainnya. Malware sering menyamar sebagai file biasa, atau tertanam dalam file yang tak berbahaya.

Penanganan Malware adalah suatu bentuk usaha mempertahankan diri dalam rangka mengamankan informasi maupun segala hal yang berhubungan dengan pengertian asset maupun resources teknologi informasi.

1.1 TUJUAN

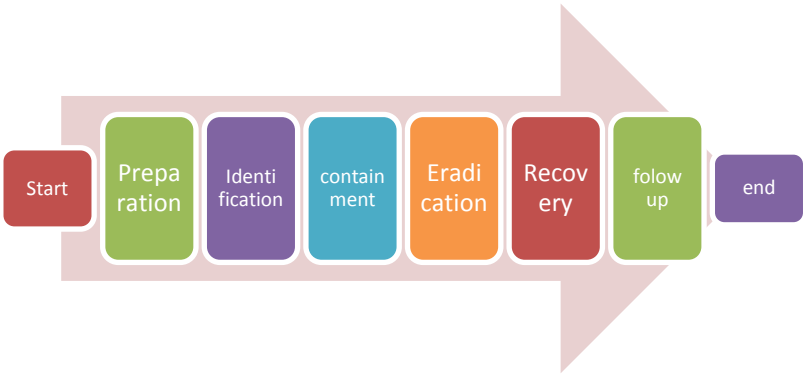
Panduan ini dimaksudkan untuk membantu organisasi memahami tentang penanganan Penanganan insiden malware yang dilakukan dengan tepat dan cepat, akan sangat bermanfaat untuk mengurangi resiko yang diakibatkan oleh serangan malware. Ancaman yang ditimbulkan oleh malware dan resiko yang terkait dengan insiden malware akan sangat berdampak bagi suatu organisasi/institusi. Selain itu juga berguna untuk memberikan informasi tentang kategori utama dari malware, dan menyediakan bimbingan mengenai tindakan praktis pada dunia nyata untuk mencegah insiden malware.

1.2 RUANG LINGKUP

Dokumen ini dibuat untuk staf keamanan komputer dan manajer program, staf dukungan teknis dan manajer, tim respon insiden keamanan komputer, dan administrator sistem dan jaringan, yang bertanggung jawab untuk mencegah, mempersiapkan, atau menanggapi insiden malware. Beberapa bagian dari panduan ini juga ditujukan untuk pengguna akhir yang mencari pemahaman yang lebih baik dari ancaman malware dan tindakan yang dapat diambil untuk mencegah insiden dan menanggapi insiden lebih efektif.

BAGIAN 2 :
LANGKAH PENANGANAN INSIDEN MALWARE

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



Gambar 1 : Tahap-tahap penanganan insiden

2.1 Tahap Persiapan (Preparation)

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

Penyiapan dokumen-dokumen yang dibutuhkan, yaitu

i. Dokumen Kebijakan dan Prosedur

Suatu dokumen kebijakan biasanya menguraikan persyaratan tertentu atau aturan yang harus dipenuhi. Suatu dokumen prosedur adalah dokumen yang memandu pengguna secara teknis dalam proses (langkah demi langkah) tentang cara untuk mencapai persyaratan yang telah ditetapkan dan diuraikan dalam dokumen kebijakan. Beberapa kebijakan, yang sering digunakan untuk membantu dalam mencegah masuknya malware dan menghentikan penyebaran itu adalah,

a. Kebijakan Keamanan:

Sebuah kebijakan keamanan adalah dokumen tingkat tinggi dari top manajemen yang menunjukkan pendekatan organisasi terhadap keamanan informasi. Menurut standar ISO 27001 Keamanan Informasi, dokumen harus memberikan arahan dan dukungan dari manajemen untuk keamanan informasi sesuai dengan kebutuhan bisnis, hukum, dan peraturan yang relevan.

b. Kebijakan penggunaan Antivirus:

Kebijakan Antivirus adalah kebijakan yang mendefinisikan apa yang harus dan tidak boleh dilakukan dari para pengguna mengenai perangkat lunak antivirus yang mereka gunakan, termasuk bagaimana cara mengelolah perangkat lunak antivirus. Suatu prosedur manual harus mengikuti kebijakan ini, yang bisa membimbing pengguna tentang cara memeriksa versi dan definisi virus baru, dan bagaimana untuk menjaga perangkat lunak agar selalu harus diperbaharui (update). Hal ini juga harus memandu pengguna tentang cara untuk mengidentifikasi apakah antivirus tersebut bekerjabenar atau tidak.

c. Kebijakan penggunaan yang diperbolehkan (acceptable use)

Kebijakan ini berisi tentang sesuatu yang diperbolehkan atau tidak diperbolehkan, termasuk pemanfaatan semua sumber daya organisasi. Hal ini akan membantu pencegahan terhadap masuknya dan penyebaran dari malware, karena para anggota organisasi akan peduli terhadap tindakannya yang mungkin secara sengaja maupun tidak menimbulkan resiko bagi sumber daya organisasi, kebijakan penggunaan Removable media (flashdisk, CD/DVD), piracy software (gratis/bajakan)

d. Kebijakan penggunaan Internet

Sebuah Kebijakan Penggunaan Internet adalah sebuah kebijakan yang mendefinisikan bagaimana pengguna diarahkan dalam menggunakan akses internet yang disediakan oleh organisasi. Hal ini juga harus menentukan tindakan disiplin apa yang akan dikenakan apabila terjadi pelanggaran. Hal ini membantu mencegah pengguna dari browsing situs yang tidak sah dan mengunduh perangkat

lunak dari Internet,yang bias menjadikan pintu masuk malware ke dalam intranet organisasi/institusi

e. Kebijakan penggunaan Email

Kebijakan penggunaan email harus menentukan bagaimana email perusahaan digunakan secara aman. Hal ini harus mencegah pengguna dari menggunakan email perusahaan untuk penggunaan pribadi, termasuk penerbitan dan pendaftaran pada kelompok dan forum di internet. Hal ini akan mengurangi jumlah spam yang diterima oleh mail server organisasi dan juga membantu mengurangi probabilitas pengguna menerima konten berbahaya melalui email mereka.

f. Kebijakan penggunaan laptop

Kebijakan laptop harus menentukan bagaimana pengguna diarahkan untuk mengetahui tindakan apa saja yang bisa dan boleh dilakukan oleh pengguna dalam menggunakan laptopnya. Hal ini juga harus menetapkan langkah apa yang perlu diambil pengguna untuk memastikan keamanan, tidak hanya keamanan fisikdari laptop itu sendiri, tetapi juga dari informasi yang terkandung didalamnya.

g. Kebijakan melakukan Backup

Kebijakan melakukan backup harus mendefinisikan apa, kapan, dan bagaimana informasi harus dibackup. Hal ini harus mendefinisikan secara jelas mengenai jenis informasi dan kapan waktu proses backup harus dilakukan, dan bagaimana cara untuk melakukannya. Backup yang baik kadang-kadang bisa menjadi satu-satunya cara untuk pulih dari kerusakan serius yang disebabkan oleh infeksi malware.

h. Kebijakan pelaporan dan mekanisme pelacakan insiden

Keberhasilan di balik rencana penanganan insiden adalah memiliki mekanisme pelaporan dan pelacakan yang mudah digunakan dan efektif. Pengguna umumnya mengharapkan mekanisme pelaporanyang dapat dengan mudah dipahami dan menangkap insiden dengan informasi sesedikit mungkin. Pengguna juga harus bisa memberikan tingkat prioritas formal yang dapat divalidasi dan diubah, jika diperlukan oleh helpdesk atau tim keamanan pusat. Nama, nomor telepon dan alamat email untuk menghubungi dalam kasus terjadinya suatu aktivitas berbahaya yang dicurigai harus diberikan melalui semua media komunikasi seperti situs intranet perusahaan, buletin dan catatan kecil di sekitar workstation pengguna.

i. Prosedur dan formulir penanganan insiden

Organisasi harus memiliki rencana dan prosedur penanganan insiden yang tepat dan bisa dilakukan di tempat organisasi berada. Organisasi harus menyediakan form yang dapat digunakan untuk mencatat dan merekam semua kejadian secara rinci, selama penanganan insiden pada semua tahapan.

j. Dokumen tentang audit

Catatan dari audit secara berkala pada sistem informasi akan membantu dalam mengungkap setiap aktivitas berbahaya yang ada. Catatan ini dapat mengungkap kegiatan yang dilakukan pengguna pada sistem yang mungkin tidak disadari. Tim audit biasanya terdiri dari personil terlatih yang tahu apa yang harus dicari.

k. Dokumen profil perangkat lunak pada proses bisnis

Disarankan untuk memiliki profil dari semua perangkat lunak dan proses-proses yang harus berjalan pada sistem berdasarkan proyek atau departemen. Hal ini dapat membantu dalam identifikasi secara cepat dari keberadaan perangkat lunak atau proses yang tidak diketahui yang mungkin terinfeksi dari malware .

l. Dokumen pengetahuan

Sebuah dokumentasi rinci dari pengetahuan dasar yang baik dan mudah mendapatkannya, dapat menghemat banyak waktu ketika insiden terjadi. Ketika sebuah insiden terjadi, semua dokumentasi mengenai penanganan kejadian harus ditambahkan ke dokumen basis pengetahuan. Jadi jika insiden yang sama terjadi lagi, proses penanganannya akan menjadi lebih cepat karena sudah ada catatan cara penanggulangannya. Hal ini akan menghemat banyak waktu yang akan dikonsumsi dalam analisis ulang insiden tersebut. Sebuah template Root Cause Analysis yang dapat menangkap sebagian besar rincian insiden harus disiapkan dan digunakan.

ii Penyiapan Teknologi yang akan dipakai

Berbagai infrastruktur teknis & perangkat lunak yang dapat mencegah malware termasuk Antivirus Scanner Online, URL dan emailfilter, Virus Submissions URL, Mesin Uji (mesin nyata dan mesin virtual), utilitas dari sistem operasi dan peralatan Reverse Engineering, harus disiapkan guna penanganan insiden malware

a. Filter URL dan email :

Hampir semua organisasi saat ini terhubung ke internet untuk berbagai tujuan termasuk email. Koneksi ke internet dan email

adalah jalan yang paling umum bagi malware untuk memasuki jaringan intranet perusahaan. Entri tersebut harus ditolak pada perimeter jaringan, sehingga setiap lalu lintas berbahaya dapat dihentikan sebelum mereka memasuki jaringan (LAN) perusahaan. Filter URL dapat membantu dalam mencegah pengguna dari mengunduh file dari internet yang mungkin berisi program tersembunyi yang berbahaya. Penyaringan terhadap email juga harus dilakukan untuk menyaring setiap email yang rentan membawa lampiran berbahaya.Terdapat berbagai alat gratis dan komersial untuk penyaringan URL. Squid adalah salah satu yang populer dan stabil, merupakan perangkat lunak open source pada web proxy yang mendukung penyaringan URL. Squid Guard adalah tool dapat digunakan untuk menyederhanakan tugas penyaringan URL. Tool ini adalah 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. Berbagai blacklist juga dapat digunakan untuk melakukan penyaringan URL.

b. Pembatasan Internet menggunakan daftar

Salah satu cara termudah untuk melakukan penyaringan URL yang baik adalah dengan menggunakan daftar (list), terdapat dua jenis daftar yaitu, blacklist dan whitelist. Blacklist adalah daftar, yang berisi semua URL atau situs yang dilarang. Whitelist adalah daftar yang berisi semuaURL atau situs yang diizinkan. Keduanya dapat disebut sebagai 'Web ACL'. Dalam lingkungan terbatas dan aman, dianjurkan untuk menggunakan whitelist. Namun, untuk menciptakan whitelist, pertama semua URL yang dibutuhkan untuk menjalankan bisnis harus di identifikasi. Jika daftar ini terbatas, maka menggunakan whitelist adalah cara terbaik. Tetapi jika pengguna menggunakan internet melalui mesin pencari, maka whitelist tidak dapat diciptakan. Dalam kasus seperti blacklist harus dibuat, daftar ini harus berisi semuaURL yang akan

diblokir. Daftar ini pertama kali diperiksa oleh web proxy sebelum diijinkan untuk akses dan jika URL tidak ditemukan dalam daftar, berarti dapat diperbolehkan akses.

c. Penenonaktifkan perangkat removable

Sebagian besar pembuat malware saat ini telah mengembangkan teknik untuk menyalin malware ke perangkat removable dan mereka jalankan segera setelah alat terkoneksi ke sistem. Disarankan untuk menonaktifkan semua perangkat removable, jika tidak keperluan. Hal ini dapat dilakukan dengan melepas kabel koneksi pada motherboard, menonaktifkan port onboard, (USB,Bluetooth, IR) di BIOS dan juga pada tingkat OS dengan memanfaatkan GPO(Group Policy Objects) pada windows dan pembatasan akses dalam Linux. Kadang-kadang menonaktifkan USB port pada tingkat BIOS mungkin tidak tepat, jika sistem menggunakanUSB keyboard dan mouse. Masalah ini dapat diatasi dengan menggunakan pembatasan tingkat OS, terdapat beberapa produk yang diciptakan untuk tujuan ini (seperti Pointsec, Safend, Safeboot), yang memiliki efisiensi dan fitur yang jauh lebih baik daripada metode dengan memblokir seperti yang dibahas atas.

d. Hash sistem file :

Langkah penting lainnya dalam tahap persiapan adalah koleksi hash untuk file-file yang penting, terutama file sistem. Biasanya, jika mesin berperilaku tidak normal atau dicurigai terinfeksi dengan malware, file yang dimodifikasi dapat dideteksi dengan membandingkan hash sistem file dengan hash yang asli. File-file juga dapat diperiksa untuk setiap infeksi malware dengan menggunakan layanan online scan antivirus yang telah dikenal atau dapat pula menyampaikan laporan kepada vendor antivirus untuk dilakukan analisis.

e. Intrusion Detection System berbasis host

Salah satu cara mudah untuk memeriksa setiap perubahan pada file system adalah dengan menggunakan Intrusion Detection System(IDS) berbasis host. IDS ini awalnya menghitung nilai hash dari semua file sistem dan menyimpannya didatabase. Hash dari file tersebut berubah setiap kali system melakukan modifikasi pada file. Dengan cara ini setiap perubahan tidak sah dapat diidentifikasi. IDS juga memeriksa setiap proses tersembunyi, mengurai log untuk setiap aktivitas yang mencurigakan. Ada banyak perangkat lunak IDS baik yang free maupun komersial. Perangkat lunak open source seperti Samhain, OSSEC dan Osiris adalah beberapa contoh dari IDS berbasis Host.

f. Antivirus

Organisasi harus memiliki perangkat lunak antivirus yang tersedia dilingkungannya, terutama untuk semua sistem yang memiliki koneksi internet atau perangkat removable (USB , DVDRW drive dll) yang aktif. Dalam hal ini dianjurkan untuk menggunakan model client-server yang jauh lebih mudah dalam hal pengelolahan. Status kerja dari antivirus pada client, instalasi pada client secara remote, dan pemindaian jarak jauh pada system adalah beberapa keuntungan pada model menggunakan solusi berbasis server.

g. Deteksi Antivirus Online

Ada dua jenis scanner antivirus secara online, masing-masing untuk tujuan yang sedikit berbeda.

1. Scanner File: Setelah file berbahaya atau malware file yang terinfeksi diidentifikasi, dapat dipindai dengan menggunakan beberapa mesin antivirus yang tersedia secara online. Hal ini akan berguna jika malware tidak dapat diidentifikasi oleh mesin antivirus yang dimiliki. Bisa juga terjadi suatu situs scan

online menyediakan scan gratis dengan menggunakan beberapa mesin antivirus, sehingga jika salah satu mesin tidak mengenali, maka mesin yang lain bisa mengenali malware, karena anti virus hanya dapat mendeteksi jenis malware tertentu yang ada pada waktu tertentu. Jika malware terdeteksi oleh salah satu mesin antivirus, maka penanganan insiden menjadi mudah.

2. Sistem Scanner: berguna untuk memindai seluruh sistem dari kehadiran malware. Hal ini berguna, jika sistem benar-benar terinfeksi dan instalasi perangkat lunak tidak memungkinkan. Hal ini dapat dilakukan untuk mengidentifikasi malware atau memeriksa keberhasilan proses pemberantasan. Pada metode ini, mesin antivirus melakukan download yang diikuti oleh file definisi dari virus. Ini akan dilakukan secara otomatis menggunakan ActiveX teknologi.

h. Virus Submissions URL:

Jika malware baru terdeteksi namun tidak dapat diidentifikasi atau dihapus, bisa dikirimkan ke laboratorium penelitian antivirus untuk analisis. Jika setidaknya salah satu mesin antivirus pada layanan online mendeteksi malware, maka akan otomatis dikirim ke semua laboratorium penelitian mesin antivirus lain untuk analisis.

i. Virus Removal Tools:

Komponen lain yang harus disediakan dalam penanganan insiden malware adalah tool dari berbagai vendor antivirus untuk menghapus malware. Tool penghapus virus bisa lebih efektif, efisien, dan mudah untuk bekerja daripada mesin antivirus. Namun, tool tersebut sebagian besar hanya bekerja terbatas pada satu keluarga malware. McAfee Stringer adalah alat removal untuk suatu kelompok malware.

j. Mesin Uji

Mesin uji adalah suatu sistem yang idealnya terisolasi, dimana malware diperbolehkan untuk menyerang dan secara bersamaan atau dikemudian akan dianalisis. Perangkat lunak virtual mesin seperti VMWare, MS VPC, Xen bisa digunakan untuk membuat mesin virtual untuk melakukan analisis terhadap malware. Virtual mesin menghemat banyak waktu dalam menciptakan laboratorium uji dan juga dalam mengembalikan sistem ke keadaan sebelum terinfeksi. Namun, memiliki mesin uji secara fisik juga dianjurkan karena sebagian besa malware canggih menggunakan teknik deteksi yang sama seperti pada mesin virtual. Jika malware cukup canggih dan dapat mengidentifikasi mesin virtual, kemungkinan dapat menjadi aktif dan dapat merusak mesin virtual. Hal ini dapat diatasi dengan baik menggunakan “Tweaking mesin virtual” 'atau dengan melakukan patching terhadap malware. Jika langkah-langkah itu gagal, satu-satunya pilihan adalah dengan menggunakan mesin fisik. Untuk membuat pekerjaan lebih mudah, sebuah solusi untuk membuat image disk to disk seperti Symantec Ghost akan sangat berguna. Pekerjaan menyiapkan laboratorium dan mengembalikan sistem ke keadaan bersih seperti semula hanya memerlukan waktu beberapa menit dibandingkan dengan waktu kerja yang dibutuhkan dalam menginstal sistem operasi, driver, dan alat-alat utilitasnya.

k. Utilitas Sistem Operasi:

Ketika wabah malware terjadi, program utilitas dapat digunakan dalam sistem operasi yang lumpuh. Dalam situasi seperti itu, sumber non-terinfeksi bisa sangat membantu. Operasi asli utilitas bersama dengan utilitas pihak ketiga dapat disalin pada media yang hanya memiliki fungsi baca seperti CD-ROM atau DVD-ROM, sehingga tidak terinfeksi ketika dijalankan. Untuk Microsoft Windows, SysInternals host

adalah utilitas yang berdaya kuat dan sederhana. Utilitas ini dapat diunduh bebas biaya dan ditambahkan ke "Utilitas Toolkit". Utilitas ini dapat digunakan untuk mengumpulkan sampel untuk analisis malware atau untuk mengidentifikasi, menampung, dan memberantas malware.

l. Reverse Engineering Tools:

Untuk analisis malware, juga perlu memiliki tool untuk melakukan reverse engineering dari sampel suatu malware. Alat analisis executable seperti PEInfo, PEiD ExeInfo, BinText bisa memberikan beberapa informasi awal mengenai cara eksekusi dari suatu malware, seperti algoritma pengemasan atau string yang digunakan oleh malware bisa ditemukan. Kemudian berbagai unpackers yang sesuai dapat digunakan untuk membongkar cara eksekusi, dan cara eksekusi yang telah terbongkar dapat dianalisis dengan alat dan teknik pembalikan (reverse). Kadang-kadang, ketika unpackers tidak tersedia atau algoritma yang digunakan tidak diketahui, maka analisis dinamis atau runtime dapat digunakan dengan menggunakan debugger. OllyDbg dan Imunitas Debugger adalah beberapa debugger terbaik yang ada pada saat ini. Softice adalah salah satu debugger alternatif yang bersifat komersial. Beberapa malware juga dilengkapi dengan deteksi rutin debugger, jika debugger terdeteksi hadir, maka malware merusak system operasi yang aktif atau pergi (beberapa mungkin menghancurkan diri) untuk menentang setiap analisis executablenya.

Banyak alat-alat bantu di SysInternal Suit pada berbagai tahap analisis. Process Explorer, Process Monitor, Berkas Monitor, Registry Monitor,Streaming adalah beberapa alat-alat dalam toolkit yang harus dimiliki oleh setiap insinyur untuk melakukan teknik reverse.

iii Penyiapan Personil (orang)

Meskipun memiliki kendali proses dan teknis yang kuat, keamanan dapat dikompromikan dengan memanfaatkan personil dan membuat mereka melakukan tindakan yang sebaliknya tidak diizinkan. Tim penanganan insiden yang terampil dan adanya matrik eskalasi merupakan komponen kunci dari startegi penanganan dan penahanan yang efektif. Sebuah tim penanganan insiden yang baik adalah sumber daya sangat berharga ketika dibutuhkan untuk menangani situasi yang mungkin timbul karena adanya malware, dengan cara yang efisien dan efektif. Sebagaimana orang adalah sumber daya organisasi utama yang akhirnya dirugikan oleh infeksi malware, kesadaran akan keamanan merupakan salah satu dari isu-isu yang perlu terus menerus dipantau dan ditingkatkan untuk perlindungan yang tepat dari berbagai serangan.

a. Kesadaran Keamanan :

Kesadaran keamanan dapat dianggap sebagai yang paling penting dari semua langkah-langkah persiapan, yang dapat membantu dalam mengidentifikasi dan mencegah sebagian besar masalah yang akan timbul. Hal ini mendidik pengguna tentang cara melindungi informasi, apa yang harus dilakukan dan apa yang tidak harus dilakukan, siapa yang harus dihubungi pada keadaan darurat dan bagaimana cara menganalisis jika mendapatkan kesulitan

b. Matrik ekskalasi penanganan insiden

Setiap organisasi harus memiliki matrik eskalasi penanganan insiden yang secara jelas mendefinisikan siapa yang harus dihubungi dalam kasus insiden. Hal ini juga menunjukkan tingkat eskalasi untuk keterlibatan lebih jauh sesuai dengan kompleksitas atau dampak dari insiden.

c. Tim Terampil Penangan Insiden

Sebuah tim penanganan insiden yang berpengetahuan dan terampil dapat mengurangi sebagian besar dampak terhadap bisnis. Tim penanganan insiden harus dimiliki pemahaman yang sangat baik dan tingkat keterampilan dalam berbagai teknologi yang digunakan oleh perusahaan. Karena, banyak perusahaan memiliki kantor-kantor cabang yang berlokasi di wilayah geografis yang berbeda, tim komando pusat dan tim lokal/regional yang sesuai sangat direkomendasikan untuk dibentuk. Tim Perintah Pusat Tentu saja, harus memandu tim lokal dalam menangani insiden .

2.2 Tahap Identifikasi

Tahap ini adalah tahap di mana identifikasi malware dan konfirmasi kehadirannya dilakukan dengan menggunakan berbagai teknik. Berikut ini adalah daftar tanda- tanda atau perilaku yang dapat diamati atau metode identifikasi yang dapat membantu mengkonfirmasi kehadiran malware. Antivirus tidak berfungsi seperti yang diharapkan :

Beberapa virus (juga dikenal sebagai virus Retro) ada yang dapat menghancurkan instalasi antivirus dengan merusak executable file, mengubah kunci registri atau merusak file definisi. Virus yang lain dapat menonaktifkan update dari signature suatu file. Salah satu cara untuk melakukan ini adalah dengan mengubah file ' hosts ' dari sistem operasi. File ini digunakan oleh system operasi untuk resolusi nama dan memiliki preferensi lebih tinggi dari resolusi nama server. Ini adalah file yang mengerjakan resolusi nama lokal host. Pada MS Windows file host ini adalah C : \ windows \ system32 \ drivers \ etc \ host, dan pada Linux adalah / etc / hosts. Sebuah virus dapat menambahkan baris ke file ini untuk menonaktifkan semua update online dari perangkat lunak apapun. Jika baris seperti "127.0.0.1 avupdate.av_vendor.com" ditambahkan oleh virus, semua permintaan ke situs web update antivirus terputus untuk sistem lokal dan selanjutnya akan gagal. Jadi jika antivirus yang ditemukan bekerja

dengan baik tapi tidak menerima pembaruan, memeriksa 'file host' apakah terdapat entri palsu mungkin membantu memecahkan masalah. Jika virus dapat menangkap permintaan ini dan membalas dengan memberikan versi file signaturnya, virus dapat dengan mudah menghindari deteksi oleh antivirus.

a. File tidak dikenal/Unusual

Virus tertentu dapat diketahui mampu untuk membuat file yang tidak biasa pada root dan sistem direktori. File-file ini memiliki nama yang mungkin menggoda pengguna untuk menyalin dan mengeksekusi pada sistem lain. Nama file mungkin menunjukkan versi berikutnya dari suatu software populer atau konten dewasa. Pada saat mengeksekusi (klik), virus membuat autorunfile dalam direktori dan drive. File-file ini meminta sistem operasi untuk menjalankan file virus untuk segera menghubungkan perangkat atau membuka folder. Dengan cara ini, jika perangkat terhubung ke komputer lain, hal itu akan dijalankan dengan segera tanpa membutuhkan eksekusi secara manual oleh pengguna terhadap file yang terinfeksi.

b. File dengan ekstensi ganda

Salah satu cara yang baik untuk mengelabui pengguna agar mengeksekusi file berbahaya adalah dengan menggunakan ekstensi ganda. Pada sistem operasi windows, hanya extensi terakhir yang dipakai sebagai file ekstensi, dan nama yang tersisa diambil sebagai nama file. Secara default, ekstensi yang dikenal disembunyikan. Jadi, esktensi yang telah dikenal seperti exe, com, scr semuanya tersembunyi. Jadi saat file ‘filename.jpg.exe’ diunduh, pengguna melihat filename.jpg sebagai file unduhan. Jika ikon diganti dengan icon jpg, pengguna bisa tertipu dengan mudah. Pengguna berpikir bahwa yang diunduh adalah file jpg dan

mencoba untuk membukanya dengan mengkliknya. Oleh karena fitur opsi 'Sembunyikan ekstensi' untuk jenis file yang dikenal dalam properti folder harus dinonaktifkan atau pengguna harus memeriksa file jika ingin melihat ekstensi yang sebenarnya dari nama file. Mekanisme infeksi jenis ini umumnya digunakan untuk meneyebarkan malware.

c. Proses tak diketahui:

Beberapa malware tertentu memulai proses dengan bantuan menetap secara siluman atau menyebar ke dalam tempat lain. Umumnya proses ini memiliki nama yang mirip dengan nama-nama proses pada sistem svchost, SMS, lsass untuk menghindari identifikasi yang mudah. Namun, proses ini dapat diidentifikasi dengan melihat pemilik proses dan dimana eksekusi proses ini melekat.

d. Kegagalan membuka utilitas sistem:

Beberapa malware mencoba untuk menyembunyikan kehadiran mereka secara diam-diam, baik mencegah pengguna untuk mengidentifikasi komponen atau mengakhiri prosesnya. Task Manager adalah utilitas sistem yang paling umum di Microsoft Windows. Alat popular lainnya adalah SysInternals Process Explorer. Kebanyakan malware (virus) menonaktifkan utilitas ini dengan menutup atau meminimalkan kerjanya, jika dibuka. Bahkan telah dikenal malware yang dapat menonaktifkan utilitas lain untuk konfigurasi sistem seperti control panel, folder options, dan bahkan command prompt. Utilitas ini akan segera ditutup, jika dibuka atau rusak sehingga mereka tidak dapat dijalankan.

Dengan cara ini setiap proses apapun yang dilakukan oleh malware, akan sulit untuk diidentifikasi. Salah satu cara yang dilakukan adalah dengan mematikan proses pemeliharaan database windows, website (URL) atau kata kunci dan mematikan

setiap proses tersebu tseperti yang diprogram oleh pembua tmalware.

e. Lambatnya Respon CPU :

Pada saat pertama kali aktivitas malware, pengguna mungkin kadang-kadang mengalami respons yang lambat dari CPU dan sistem dapat ‘hang’ selama beberapa detik. Penyebabnya adalah karena kerja malware yang paling memakan siklus CPU untuk kegiatan infeksi. Jika suatu saa ttiba-tiba komputer mulai berjalan lambat, maka ada kemungkinan mulai terinfeksi. Diperlukan proses untuk memverifikasi untuk melihat atdanya proses lain yang berjalan sehingga perilaku menjadi abnormal.

f. Sistem / Aplikasi crash :

Sistem dan aplikasi executable kadang-kadang bisa menjadi rusak karena infeksi malware. Pada saat suatu aplikasi mulai dijalankan, kemungkinan aplikasi tersebut sudah terinfeksi, sehingga kemungkinan tidak berjalan dengan baik dan bisa terjadi crash karena terjadinya perubahan kode-kode dalam programnya. Hal diatas bisa menyebabkan sistem/aplikasi menjadi crash.

g. Peringatan dari rekan :

Kadang-kadang ketika virus mencoba untuk menyebar ke sistem lain dengan tingkat keamanan yang lebih baik (pengguna dengan kesadaran keamanan yang lebih baik atau melalui pembaharuan keamanan perangkat lunak), virus tersebut mungkin terlihat. Contoh lain termasuk serangan ke sistem lain ketika file terinfeksi akan disalin ke sistem tersebut atau email dengan lampiran yang tidak diketahui diterima. Ketika sumber malware ditemukan, pengguna sumbernya seharusnya diberitahu

h. Forum keamanan informasi :

Salah satu cara untuk mengidentifikasi gejala dari malware baru adalah dengan mempelajarinya dari berbagai forum keamanan untuk malware yang baru dirilis. Jika ada gejala yang sama yang ditemukan dalam jaringan, investigasi lebih lanjut dapat dilakukan dengan informasi yang tersedia di forum.

2.3 Containment

Tahap ini merupakan fase aktif pertama yang melibatkan perubahan lingkungan untuk menghentikan atau secara harfiah mencegah penyebaran malware. Metode yang digunakan dapat mencakup mengisolasi sistem yang terinfeksi dari jaringan.

a. Izin/pemberitahuan untuk melakukan Containment

Hal pertama setelah konfirmasi keberadaan malware adalah memberitahukan kepada personil bahwa sistem komputernya telah terinfeksi, dengan diikuti untuk meminta izin yang diperlukan untuk mengisolasi sistem. Izin dari unit bisnis terkait sangat penting sebagai dampak proses isolasi dan pemilik sistem harus diberitahu tentang keadaan dan situasi yang sedang terjadi.

b. Isolasi sistem

Setelah memperolah ijin, sistem yang terinfeksi harus diisolasi. Isolasi dapat dilakukan baik secara fisik dengan memutuskan sistem (juga dapat dilakukan dengan menonaktifkan kartu jaringan), atau mengkarantina sistem dari jaringan dengan memindahkan sistem ke VLAN yang berbeda. Perlu diingat untuk menyimpan informasi koneksi jaringan pada sistem sebelum

memutuskan hubungan dari jaringan yang mungkin akan dibutuhkan dalam melakukan analisis selanjutnya.

c. Memeriksa gejala kemiripan

Setelah gejala dasar dicatat, sistem lain yang berada dalam jaringan perlu juga diperiksa untuk melihat apakah mereka menunjukkan gejala yang sama. Jika positif, maka sistem lain tersebut juga harus diisolasi dan dianalisis untuk melihat adanya keberadaan malware.

d. Melihat insiden yang pernah ada (Basis Pengetahuan)

Langkah selanjutnya setelah mengidentifikasi gejala dasar malware adalah menelusuri dokumen untuk mencari pengetahuan yang berisi insiden yang pernah terjadi di masa lalu. Jika insiden tersebut merupakan pengulangan, maka prosedur yang diikuti sebelumnya harus dieksekusi dan dianalisis secara mendalam dari setiap langkah untuk mengidentifikasi penyebab terulangnya kejadian dan memastikan apakah langkah-langkah tersebut cukup atau tidak. Jika belum, maka diperlukan perbaikan secara utuh pada prosedur.

e. Melakukan backup semua data pengguna

Sebelum memasuki fase pemberantasan, semua data pengguna yang ada diambil sebagai backup (cadangan) dan harus terus diisolasi dari backup lain yang mungkin terinfeksi dengan komponen malware. Hal ini dilakukan untuk mengembalikan data yang hilang, setelah selesainya analisis malware. Setelah analisis malware berhasil dilakukan, semua komponen malware yang terdapat pada backup dapat dihapus dan data pengguna dapat dipulihkan kembali seperti semula.

2.4 Pemberantasan

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 secara hati-hati dicatat dan executable malware diidentifikasi dan dianalisis. Setelah analisis, semua malware executables dan artefak yang ditinggalkan oleh malware akan dihapus dan lubang (holes) yang mengikuti infeksi ditambal (patch).

a. Memeriksa Integritas Sistem file

Semua file sistem diperiksa untuk melihat adanya otorisasi dan modifikasi yang tidak diinginkan (cek Integritas). Hal ini dapat dilakukan dengan membandingkan hash file saat ini dengan yang telah dicatat sebelumnya..

b. **Mengidentifikasi file baru**

Kebanyakan malware membuat file baru, yang mana dapat membantu dalampenyebaran pada system lokal, menyebar ke system lain dan mengakibatkan kesulitan dalam proses pembersihan. Untuk membasmi malware dengan benar, semua file-file ini harus diidentifikasi dan dihapus dari sistem.

c. Identifikasi gejala lain

Untuk membasmi dengan benar dan untuk mengidentifikasi infeksi dimasa depan, semua gejala malware harus diidentifikasi. Hal ini dapat dicapai dengan pengamatan yang cermat, baik pada sistem keseluruhan yang terinfeksi atau sampel (contoh) sistem ujiyang terinfeksi. Beberapa malware yang dirilis memiliki fitur untuk mendeteksi mesin virtual dan beberapa juga memiliki kemampuan untuk menolak mesin virtual. Sebagian besar malware dengan fitur seperti diatas, mematikan beberapa karakteristik mereka untuk menghindari pengungkapan gejala

mereka dari peneliti anti malware. Teknik analisis perilaku perlu dimanfaatkan untuk mengidentifikasi semua gejala malware tersebut.

d. Menganalisis file

Dalam tahap ini, executable malware yang dikumpulkan pada kegiatan sebelumnya dianalisis. Hal ini dilakukan dengan cara reverse engineering executable menggunakan disassemblers, debugger dan utilitas. Hal ini memudahkan untuk mengidentifikasi fungsi bagian dalam dari malware, dan dapat memberikan petunjuk dalam proses identifikasi dan pembersihkan malware. Hal ini juga membantu dalam menambah daftar dari gejala malware yang telah dikumpulkan selama ini.

e. Memeriksa Jaringan

Setelah semua gejala dikumpulkan, suatu mekanisme pencegahan dikembangkan dan diimplementasikan. Dengan memperhatikan gejala malware yang ada, jejak-jejak malware pada sistem lain dalam jaringan dapat teridentifikasi. Jika ditemukan, sistem lain itu juga ditangani sesuai untuk proses yang telah digunakan. Misalnya, jika suatu virus meneteskan bot atau backdoor, maka pemindaian jaringan, port yang terbuka, dan Log dari firewall yang menunjukan adanya lalu lintas yang mencurigakan, harus dianalisa.

f. Memeriksa Backup

Selanjutnya adalah mengambil backup yang dari sistem yang sedang berjalan dan memeriksanya untuk mencari jejak dari malware. Setelah memastikan bahwa sistem backup telah bersih dari walware, maka dilakukan pemulihan dan mengembalikan data-data yang telah diambil/hilang.

g. Menemukan Penyebab

Tahap ini adalah kegiatan yang paling penting dan juga merupakan salah satu kegiatan terberat dalam tahap pemberantasan. Penyebab insiden (atau infeksi) harus dapat ditemukan, sehingga insiden tidak akan terjadi di masa depan. Untuk melakukan hal ini, log sistem, server proxy dan perangkat perimeter harus diperiksa sebagaimana mestinya. Sistem log yang diperiksa termasuk event log, log antivirus dan log dari setiap kontrol keamanan lainnya (Software atau perangkat). Proxy log dapat digunakan untuk memeriksa apakah sumber infeksi adalah dari internet dengan meninjau catatan URL yang telah dikunjungi. Log server email dapat diperiksa untuk mengetahui apakah malware disebarkan melalui email dalam jaringan. Log dari peralatan perimeter diperiksa untuk mengetahui titik masuk malware ke dalam jaringan.

h. Meningkatkan Pertahanan

Setelah penyebab infeksi ditemukan, langkah selanjutnya adalah memperkuat pertahanan dan mencegah malware supaya tidak masuklagi. Hal ini bias dilakukan dengan memodifikasi aturan akses di perangkat perimete rjaringan, penyaringan email, memblokir URL tertentu atau jenis file dan menghapus akses keperangkat tertentu seperti USB dan DVD.

2.5 Pemulihan

Pada tahap ini, sistem yang telah pulih divalidasi oleh pengguna aplikasi dan suatu keputusan mengenai kapan memulihkan sistem operasi secara lengkap akan dibuat. Sistem ini dijaga dalam pengamatan, untuk memeriksa dan memastikan komponen dari malwaret idak ada yang tersisa selama poses sebelumnya.

a. Validasi sistem

Sistem yang telah pulih, harus divalidasi terhadap kesalahan atau kekurangan konfigurasi apapun. Jika ada kekurangan pada perangkat lunak atau data yang ditemukan, maka akan ditambahkan. Sebuah tanda tangan dari pengguna harus diambil untuk mengkonfirmasikan pemulihan lengkap dan normal dari sistem.

b. Pemulihan Operasi

Setelah validasi sistem pulih selesai, pemilik sistem memutuskan kapan untuk menempatkan sistem kembali online. Rekomendasi mengenai keamanan system dapat diberikan kepada pemilik sistem. Pemilik harus mengakui rekomendasi ini melalui memo yang telah ditandatangani .

c. Pemantauan Sistem

Akhirnya aktifitas penting pada tahap pemulihan adalah melakukan pemantauan secara cermat agar sistem tidak terinfeksi kembali oleh malware. Kadang- kadang analisis yang dilakukan pada tahap sebelumnya kemungkinan tidak mengungkapkan semua executable malware yang masih terdapat dalam sistem. Executable malware yang bersifat sebagai siluman akan mencoba untuk menginfeksi sistem sekali lagi dan pemantauan secara cermat dapat membantu mengidentifikasi komponen yang tertinggal.

2.6 Tahap Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk dimasa mendatang. Fase inidapat memberikan masukan kepada tahap persiapan untuk meningkatkan pertahanan.

a. Penambahan pengetahuan dasar tentang penangan insiden

Salah satu hal penting yang harus dilakukan setelah berhasil menangani sebuah insiden adalah memperbarui pengetahuan. Catatan tentang penambahan

pengetahuan ini harus ditambahkan pada dokuman laporan dan direview oleh semua pihak yang telah berperan dalam penanganan insiden. Hal ini akan membantu dalam penanganan insiden serupa di masa depan dengan mudah, efisien, dan cepat.

b. Penciptaan signature dan inklusi antimalware

Jika suatu malware tidak dapat terdeteksi oleh antimalware, sampel malware dan analisis yang dilakukan harus dikirim ke vendor antimalware. Setelah signature dibuat, semua klien yang menggunakan antimalware harus memperbaharuinya dengan signature file yang baru, dengan harapan dapat berhasil dalam mendeteksi dan menghapus malware.

c. Pelatihan untuk tim penanganan insiden

Tim penanganan harus melatih semua tim penanganan lainnya dalam penanganan insiden malware ini. Hal ini akan membantu mereka lebih memahami proses penanganan insiden dan juga membantu dalammenanggulangi insiden serupa di masa mendatang dengan lebih terampil.

d. Memperbarui aturan penyaringan

Semua jalan masuknya malware yang diidentifikasi harus dapat diblokir untuk mencegah malware masuk ke dalam jaringan di masa depan. Hal ini dapat dilakukan dengan menambahkan aturan baru diperimeter dan perangkat penyaringan lainnya (seperti filter URL, filter email, IDS).

e. Pendidikan bagi penggunan dalam identifikasi Malware

Semua informasi mengenai identifikasi malware sebaiknya diterbitkan dalam buletin perusahaan. Dengan cara ini, pengguna akan menyadari gejala malware yang berbeda dan dapat melaporkan hal yang sama ke pihak helpdesk, jika melihat ada gejala yang mencurigakan

f. Peningkatan Pertahanan

Setelah penanganan selesai, Root Cause Analysis digunakan untuk menguatkan berbagai kontrol keamanan yang terdapat dalam perusahaan. Tim teknis dapat dibuat peduli dan menyadari terjadinya gejal amalware yang sama pada pemeriksaan entitas, tim penanganan insiden dapat diberikan insiden serupa untuk melatih diri dan manajemen dapat memperkenalkan kontrol keamanan yang baru untuk mengurangi risiko di masa depan.

LAMPIRAN A – Informatif

1. Pengertian Malware

Malware adalah singkatan dari Malicious Ware yang berarti perangkat lunak yang dirancang untuk mengganggu kerja dari sebuah sistem komputer. Perangkat lunak ini diperintahkan untuk melakukan perubahan diluar kewajaran kerja dari system komputer. Malware biasanya menyusup pada sistem jaringan komputer tanpa diketahui oleh pemilik jaringan komputer, dari jaringan komputer ini malware tersebut akan memasuki sebuah sistem komputer. Pemilik komputer juga tidak mengetahui bahwa komputernya telah disusupi oleh malware. Tujuan seseorang untuk menyusupkan program jahat bisa bermacam-macam, mulai hanya sekedar iseng ingin mencoba kemampuan, merusak data, mencuri data, sampai menguasai computer orang lain dan mengendalikannya dari jarak jauh melalui jaringan komputer.

Beragam jenis Malware

Virus:

Virus adalah sebuah program replikasi diri yang menempel pada perangkat lunak yang sah dan membutuhkan interaksi pengguna untuk berhasil menginfeksi sistem.Virus adalah sebutan untuk salah satu malware. Malware belum tentu virus, tapi virus sudah pasti malware. Virus dapat menyebar dan berkembang di dalam sistem komputer. Beberapa virus tidak akan terasa dampaknya pada komputer atau perangkat lainnya, namun ada pula virus yang sifatnya berbahaya. Karena bias memperbanyak diri, dampak yang paling terasa adalah berkurangnya ruang di memory atau hard disk perangkat dengan signifikan. Tentu ini cukup mengganggu sang pengguna.

Pencegahan:

 Menghindari membuka lampiran e-mail dari sumber yang tidak diketahui
 Menghindari pengunduhan software/file secara ilegal.
Penghapusan:
 Dengan menggunakan software Anti-Virus

Trojan Horse:
Merupakan jenis malware yang memiliki sifat seperti kuda Trojan. Trojan dapat berupa program apapun yang menyerupai program yang sah, namun didalamnya memiliki beberapa kode berbahaya. Jenis ini merupakan kode non-replikasi dan umumnya bersifat parasit karena membutuhkan sebuah program yang sah untuk menyembunyikan diri.Trojan merupakan sebuah perangkat lunak yang berdiri sendiri yang tidak menempelkan dirinya ke program lain atau menyebarkan dirinya melalui jaringan. Trojan mendapatkan nama mereka dari Trojan horse terkenal dalam mitologi Yunani. Sebuah Trojan Backdoor, setelah diinstal dapat memungkinkan hacker untuk mengakses secara remote terhadap komputer yang telah terinfeksi. Penyerang setelah itu dapat melakukan berbagai tindakan pada komputer yang terkena, dari mulai mencuri informasi sampai menggunakan komputer untuk mengirimkan SPAM.

Pencegahan:

- Menghindari untuk membuka lampiran e-mail dari sumber yang tidak diketahui
- Menghindari mengunduh software/file secara illegal
- Memastikan browser selalu dalam kondisi up-to-date
- Tidak membuka link di e-mail.

Penghapusan:

Kebanyakan trojan dapat dihapus oleh perangkat lunak anti-virus. Namun perlu diingat bahwa setelah Trojan terinstal di sistem,maka trojan akan mengunduh perangkat lunak berbahaya lainnya ke sistem anda.

Worm:

Worm adalah sebuah program replikasi diri yang menggunakan kerentanan dalam jaringan komputer untuk menyebarkan dirinya. Berbeda dengan virus komputer worm tidak perlu melampirkan sendiri ke program lain dan tidak memerlukan interaksi pengguna untuk menjalankan. Kerusakan yang disebabkan oleh worm computer tergantung pada muatan mereka. Meskipun beberapa worm hanya diprogram untuk memperbanyak diri di seluruh jaringan, mereka masih bisa mengganggu karena mereka mengkonsumsi bandwidth jaringan. Worm lain membawa muatan lebih berbahaya karena mereka bisa menciptakan backdoors untuk hacker untuk mengambil kontrol dari PC, mengubahnya menjadi sebuah "zombie" yang akan mengeksekusi perintah dari kata hacker .

Pencegahan :

- Menghindari membuka lampiran e-mail dari sumber yang tidak diketahui
- Menghindari mengunduh software / file secara ilegal
- Memastikan browser selalu up - to-date
- Tidak membuka klik link di e - mail.

Penghapusan:
Karena worm merambat melalui koneksi jaringan, penghapusan bisa menjadi rumit. Setiap mesin yang terinfeksi harus diambil dari jaringan dan dibersihkan. Setelah mesin kembali terhubung harus dipantau agar tidak terinfeksi kembali. Jika mesin terinfeksi kembali dalam waktu singkat, itu bisa berarti bahwa ada lebih banyak mesin yang terinfeksi pada jaringan .

Trapdoor:

Istilah Trapdoor dapat berarti pintu masuk alternatif ke dalam sistem. Jenis malware ini digunakan untuk memotong mekanisme keamanan yang ada dibangun menuju ke dalam sistem. Mereka umumnya dibuat oleh programmer untuk menguji fungsi kode tertentu dalam waktu yang singkat,

sehingga dalam banyak kasus, tidak sengaja tertinggal. Namun, jenis malware ini juga mungkin ditanam oleh penyerang untuk menikmati akses istimewa. trapdoors umumnya mandiri dan berjenis non-replikasi malware.

Logic Bomb:

Logic Bomb adalah jenis malware yang mengeksekusi beberapa set instruksi untuk menyerang sistem informasi berdasarkan logika yang didefinisikan oleh penciptanya. Logic bomb biasanya berupa program yang menggunakan waktu atau peristiwa yang baik sebagai pemicu. Ketika kondisi yang ditetapkan dalam set instruksi dipenuhi, kode yang berada payload dijalankan

Spyware:

Malware ini adalah jenis kode berbahaya yang digunakan untuk memata-matai kegiatan korban pada sistem dan juga untuk mencuri informasi yang sensitif dari klien. Jenis ini juga merupakan alat paling populer yang digunakan untuk melakukan pencurian identitas, yang merupakan risiko utama bagi pengguna sistem publik online tanpa adanya jaminan keamanan.

Spyware adalah perangkat lunak yang mengumpulkan informasi tanpa persetujuan pengguna dan melaporkan hal ini kepada pembuat perangkat lunak. Jenis informasi yang dikumpulkan benar-benar tergantung pada apa yang pembuat spyware inginkan. Informasi ini kemudian dapat dijual kepada pengiklan yang dapat mengirimkan lebih banyak iklan bertarget. Mereka juga bisa mendapatkan informasi seperti username, password dan informasi sensitif lainnya. Mereka menggunakan informasi ini untuk mencuri identitas dan uang.

Pencegahan:

- Menghindari membuka lampiran e-mail dari sumber yang tidak diketahui
- Menghindari mengunduh software / file secara ilegal
- Memastikan browser selalu up-to-date

 Tidak membuka link dalam e-mail yang tidak diminta.

Penghapusan:

Menggunakan Anti-Virus/Anti-Spyware software (saat ini sebagian besar perangkat lunak anti-virus dapat menghapus spyware)

Rootkit:

Rootkit adalah kumpulan program yang digunakan untuk mengubah fungsi system operasi standar dengan tujuan untuk menyembunyikan kegiatan berbahaya yang sedang dilakukan olehnya. Malware ini umumnya menggantikan operasi dari utilitas umum seperti kernel, netstat, ls, ps dengan set dari program mereka sendiri, sehingga salah satu aktivitas yang berbahaya dapat disaring sebelum menampilkan hasilnya pada layar.

Pencegahan:

 Menghindari membuka lampiran e-mail dari sumber yang tidak diketahui
 Menghundari mengunduh software/file secara ilegal
 Memastikan browser selalu up-to-date
 Tidak membuka link di e-mail.

Penghapusan:
Terdapat tool anti-rootkit yang tersedia, juga beberapa solusi anti-virus dapat mendeteksi dan menghapus rootkit.

Bot dan Botnet:

Sebuah bot adalah program yang melakukan tindakan berdasarkan instruksi yang diterima dari tuannya atau controller. Jaringan yang digunakan oleh bot tersebut disebut botnet. Karena ini adalah program yang bersifat otonom, maka sering digunakan dalam lingkungan komunitas tertutup untuk menyelesaikan banyak tugas berbahaya dengan

menggunakan teknik remote kontroler (dikendalikan dari jauh).

Pencegahan:

Bot-agen (perangkat lunak yang mengubah suatu komputer menjadi bot) didistribusikan dalam beberapa cara, salah satu metode distribusi yang paling umum untuk bot-agen adalah melalui lampiran e-mail. Inilah sebabnya mengapa penting untuk tidak membuka lampiran dari sumber yang tidak diketahui. Bot-agen juga dapat dimasukkan dalam software ilegal/file. Jadi metode yang baik untuk mencegah bot- agen adalah untuk tidak berpartisipasi dalam mengunduh materi ilegal. Juga menjaga browser internet Anda up-to-date untuk mencegah Drive-by-download

Penghapusan:

Bot-agen dapat dikenali dan dihapus oleh perangkat lunak Anti-Virus (jadi pastikan perangkat lunak Anti-Virus Anda selalu up to date).

2. Cara kerja Malware

Secara garis besar, malware memiliki 4 tahap siklus hidup, yaitu

a.Dormant phase (Fase Istirahat/Tidur)

Pada fase ini malware tidaklah aktif. Malware akan diaktifkan oleh suatu kondisi tertentu, semisal tanggal yang ditentukan, kehadiran program lain/dieksekusinya program lain, dan sebagainya. Tidak semua malware melalui fase ini

b.Propagation phase (Fase Penyebaran)

Pada fase ini malware akan mengkopikan dirinya kepada suatu program atauke suatu tempat dari media storage (baik hardisk, ram dsb). Setiap programyang terinfeksi akan menjadi hasil “klonning” dari malware

tersebut(tergantung cara malware tersebut menginfeksinya)

c.Trigerring phase (Fase Aktif)

Di fase ini malware tersebut akan aktif dan hal ini juga di picu oleh beberapakondisi seperti pada Dormant phase.

d.Execution phase (Fase Eksekusi)

Pada Fase inilah malware yang telah aktif tadi akan melakukan fungsinya. Seperti menghapus file, menampilkan pesan-pesan, dan sebagainya.

Beberapa sumber penyebaran dari malware

a.Disket, media storage R/W

Media penyimpanan eksternal dapat menjadi sasaran empuk bagi malware untukdijadikan media. Baik sebagai tempat menetap ataupun sebagai media penyebarannya. Media yang bisa melakukan operasi R/W (read dan Write) sangat memungkinkan untuk ditumpangi malware dan dijadikan sebagai media penyebaran.

b.Jaringan (LAN, WAN,dsb)

Hubungan antara beberapa komputer secara langsung sangat memungkinkan suatu malware ikut berpindah saat terjadi pertukaran/pengeksekusian file/programyang mengandung malware.

c. Halaman web (internet)

Sangat mungkin suatu situs sengaja di tanamkan suatu malware yang akan menginfeksi komputer-komputer yang mengaksesnya.

d. Software yang Freeware, Shareware atau bahkan Bajakan

Banyak sekali malware yang sengaja ditanamkan dalam suatu program yang disebarluaskan baik secara gratis,

atau trial version yang tentunya sudah tertanam malware didalamnya.

e. Attachment pada Email, transferring file

Hampir semua jenis penyebaran malware akhir-akhir ini menggunakan email attachment dikarenakan semua pemakai jasa internet pastilah menggunakan email untuk berkomunikasi, file-file ini sengaja dibuat mencolok/menarik perhatian, bahkan seringkali memiliki ekstensi ganda pada penamaan filenya.

3. Pencegahan terhadap malware

Bagian ini menyajikan rekomendasi untuk mencegah insiden malware dalam sebuah organisasi.

a. Email merupakan salah satu perantara malware yang paling banyak digunakan. Berikan perhatian lebih pada SPAM email. Jangan membuka spam email dari sumber/pengirim yang tidak jelas.Itulah alasan kenapa penyedia layanan email seperti Gmail, Yahoo mail atau Hotmail menyediakan folder SPAM. Email yang dicurigai dapat merusak komputer karena mengandung virus, malware atau sejenisnya akan masuk ke folder tersebut. Apabila dalam email yang dibuka terdapat lampiran file (attachments) tidak usah diunduh jika tidak dikenal pengirimnya atau melakukan scan sebelum membuka file tersebut.
b. Internet menjadi tempat terbesar untuk menyebarkan malware. Tidak mudah tergiur dengan pop-up iklan yang muncul tiba-tiba dan menyebutkan anda memenangkan suatu hadiah/undian. Tutup pop-up tersebut atau sekalian saja meninggalkan situs web tersebut. Beberapa program antivirus menyediakan toolbar pencarian khusus seperti AVG Link Scanner, yang dilengkapi kemampuan scan situs web hasil pencarian google. Ini berguna untuk mencegah anda mengunjungi website yang terinfeksi malware.
c. Melakukan scan terlebih dahulu sebelum menyalin (copy) file dari perangkat penyimpanan seperti USB flash disk

dan memory card. Menggunakan klik kanan kemudian menekan 'Open' untuk melihat isi flash disk, cara ini lebih aman dibandingkan melakukan double click. Menghindari membuka file atau folder mencurigakan yang ada di dalam flash disk. Contohnya file/folder dalam bentuk shortcut.

d. Menginstall antivirus yang bagus dan melakukan update program secara berkala. Tujuannya adalah supaya antivirus bisa mengenali varian virus baru sehingga ampuh mencegah penyebaran infeksi pada komputer. Memasang juga antivirus lokal sebagai software pendamping karena antivirus lokal lebih mengenali varian virus buatan lokal. Jika program antivirus yang digunakan tidak memiliki fitur anti-spyware, menginstall software anti-spyware untuk perlindungan lebih maksimal.
e. Berhati-hati jika mengunduh file dari situs yang menyediakan file illegal seperti cracks, serials, warez. Situs web seperti ini umumnya dijadikan tempat penyebaran virus, worm dan trojan.
f. Selalu membuat jadwal secara teratur untuk update dan scan. Penjadwalkan secara teratur untuk update dan scan system akan membantu meminimakan kerusakan apabila tanpa sepengetahuan ternyata komputer terinfeksi trojan. Mencoba mengikuti trend arah perkembangan malware. Semakin hari, malware semakin berkembang dan semakin intrusif dalam ide dan skema serangan. Karena itu sebaiknya mempersenjatai diri dengan update info-info terkini. Tidak perlu tahu terlalu mendetail, cukup mengenal secara general dan mengerti trend penyebaran.
g. Selalu memeriksa removable media yang di hubungkan ke komputer. Malware sering menggunakan media removable misal USB FD, External HDD dan media storage lainnya sebagai media penyebaran. Mereka juga menggunakan fasilitas Autorun windows untuk aktifasi otomatis begitu removable media dihubungkan ke komputer.
h. Mencari situs yang memiliki akses online ter-enkripsi untuk transaksi penting, misal perbankan atau jual-beli. Menggunakan website terpercaya dalam melakukan

transaksi dengan mode terenkripsi/enkapsulasi, misal HTTPS/SSL. Di dunia interne yang luas, data dan paket informasi hilir mudik sebagian besar tanpa terlindungi dan hanya berupa plain text. Orang–orang jahat yang bisa melakukan tap, umumnya bisa membaca isi paket tanpa kesulitan. Karena itu menggunakan situs terenkripsi yang mengubah paket/data menjadi string tak terbaca yang hanya bisa dibuka oleh penerima. Orang jahat pun akan mengalami kesulitan membuka data yang diterima, mereka akan memerlukan waktu lebih banyak untuk membongkarnya. Perkembangan dunia internet, hacking dan cracking, memungkinkan suatu saat bahkan metode enkripsi terbaik sekalipun untuk dijebol. Tetapi diharapkan pelaku kejahatan memerlukan waktu lebih banyak untuk melakukan satu aksi kejahatan.

i. Selalu mengambil sikap paranoid dan berhati–hati ketika berada di dunia Internet. Hal itu berguna untuk mengantisipasi kemungkinan menjadi korban phising (pencurian data), penipuan ataupun pemerasan. Memperhatikan dengan seksama website yang dikunjungi, memilih website yang terpercaya, lengkap informasinya, dan membimbing anak-anak untuk mengakses website yang aman dan tidak menampilkan iklan–iklan tak wajar untuk usianya. Jika perlu, menggunakan content filtering untuk akses internet.
j. Melakukan penyaringan atas informasi dan data yang di terima. Dunia internet yang amat luas sehingga memungkinkan informasi mengalir demikian cepat. Melampaui batas–batas negara dan perundangan. Tapi, tidak semua informasi dan data dapat dipercaya, menggunakan selalu akal sehat, rasio dan pemikiran yang matang ketika melakukan justifikasi. Mengumpulkan data sebanyak mungkin lalu membandingkan seobjektif mungkin. Mematangkan dan menetralkan kedewasaan berpikir.
k. Tidak mematikan firewall dalam keadaan komputer aktif online terhubung ke internet. Mematikan antivirus untuk sementara waktu masih bisa ditolerir ketika ada aplikasi yang berbenturan. Tetapi mematikan firewall untuk komputer yang terhubung ke LAN/Internet adalah hal

yang tidak disarankan. Karena dalam hitungan detik saja, kelemahan OS Windows (OS Vulnerability) yang terekspos akan dijadikan tunggangan maut Trojan–trojan untuk masuk ke dalam sistem.

l. Tidak cepat percaya dengan mail yang diterima, memeriksa dengan baik sebelum membuka lampiran dan tidak sembarangan memberikan alamat email ke sembarang website. Mailware juga menyebar cepat melalui e-mail. Biasanya berupa lampiran atau autorun script. Karena itu tidak cepat mempercayai email yang masuk, apalagi dari pengirim yang tidak dikenal.