INDONESIA DARURAT MALWARE

OLEH INFALTECH

LATAR BELAKANG

Bahaya Trojan

Bahaya malware perusak sistem

Tantangan Antivirus lokal pada ancaman malware

Bahaya Trojan

Begitu banyak laporan bahkan kejadian di tahun 2014 hingga kini , yang melaporkan kejadian kehilangan data ataupun mengalami pemerasan pada file yang terjangkit/terinfeksi atau terengkripsi oleh malware pencuri bahkan perusak data ini , yang dikenali dengan sebutan trojan.

Tidak hanya merusak sistem trojan ini juga melakukan pemerasan bagi yang terjangkit oleh seranganya , dengan cara implementasi pada sebuah file ,baik berupa dokumen dan aplikasi pada sistem, dan juga mampu meregenerate sebuag virus baru yang akan menginvasi sistem.

Bagaimana cara penyebaran trojan ini ? . Tentu banya vulnerable/kerentanan yang bisa di lakukan dalam memasuki sistem, baik dengan cara promosi melalui pengiriman email melalui ads/periklanan tentu saja kerentanan itu begitu mudah di lakukan terlebih lagi jika pengguna tersebut adalah pengguna awam.

Bahaya Malware perusak

Malware perusak ,sebuah virus yang melakukan invasi dengan cara lebih mudah dengan kerentanan tanpa mengalami kesulitan, malware ini mampu juga melakukan impelemntasi kepada file data app dan dokumen,

Mengapa dikatakan perusak? ,malware ini menginfeksi file aplikasi pada sistem merusak sistem secara menyeluruh.

Mengapa dikatakan malware ? . Malware adalah sebuah program *diciptakan oleh seseorang dengan tujuan jahat. Sebenarnya Malware itu adalah sebuah software atau program komputer, namun Malware dibuat dengan tujuan untuk merugikan orang lain. Malware dapat mengubah data (menghapus, menyembunyikan, dan mencuri), menghabiskan bandwith dan juga sumber daya lain tanpa seijin pemilik komputer yang tentunya akan merugikan orang lain.*

Malicious software juga memiliki berbagai jenis , worm , virus ,spyware bahkan trojan sekalipun ... ,

Tantangan Dev. Antivirus lokal

Sering timbul pertanyaan di berbagai grup media sosial dan forum di berbagai kalangan malware test and research , bahwasannya memakai av lokal menyelesaikan sebuah invasi terhadap serangan malware tidak sepenuhnya bisa diselesaikan, Mengapa ? Fitur dan removal terkadang di andalkan namun tergantung pengguna lagi , jika pengguna tidak terlalu memahami bagaimana cara menggunakan removal tools atau antivirus tersebut , singkatnya pengguna dapat menggunakan sebuah removal malware tool yang sudah sepaket bukannya terpisah dan memerintah secara manual... terkadang dev.antivirus harus mengambil keberanian untuk menindak si malware . Misalkan harus ke safe mode boot, padahal malware tersebut bisa di unload di prosess yang aktif ... . Tapi tantanganya lagi jika si malware lebih mampu memasuki kerentanan sistem yang lebih dalam , mau tidak mau dev. Antivirus harus melakukan safe mode secara paksa baik melalu perintah sistem atau pemberitahuan sebelum menindaklanjutin tugasnya sebagai removal tools untuk malware .

Tantangan apa saja yang perlu dilakukan oleh dev.antivirus untuk tetap bisa menjadi utama pada sistem dalam removal tools , ? Berikut jawabanya

yaitu fitur yang pertama proteksi realtime yang musti di tingkatkan , misalkan teknik pendeteksian untuk mendapatkan informasi tentang file yang baru di pindahkan di unduh bahkan di exract dari arsip .

ke 2 proteksi firewall untuk mematikan koneksi port yang mencurigakan

Ke 3 yang paling penting jika malware telah menginvasi secara menyeluruh pada sistem yaitu disinfection dan service cloud untuk file sistem yang telah rusak sepenuhnya mampu untuk di perbaiki/dinormalkan kembali

Ke 4 berselancar aman di dunia maya , dengan teknologi rescue safe surf mematikan ads yang mengunduh malware otomatis , mendeteksi script jahat pada website yang di kunjungi

SEKIAN RINGKASAN PERSENTASI DARI KAMI