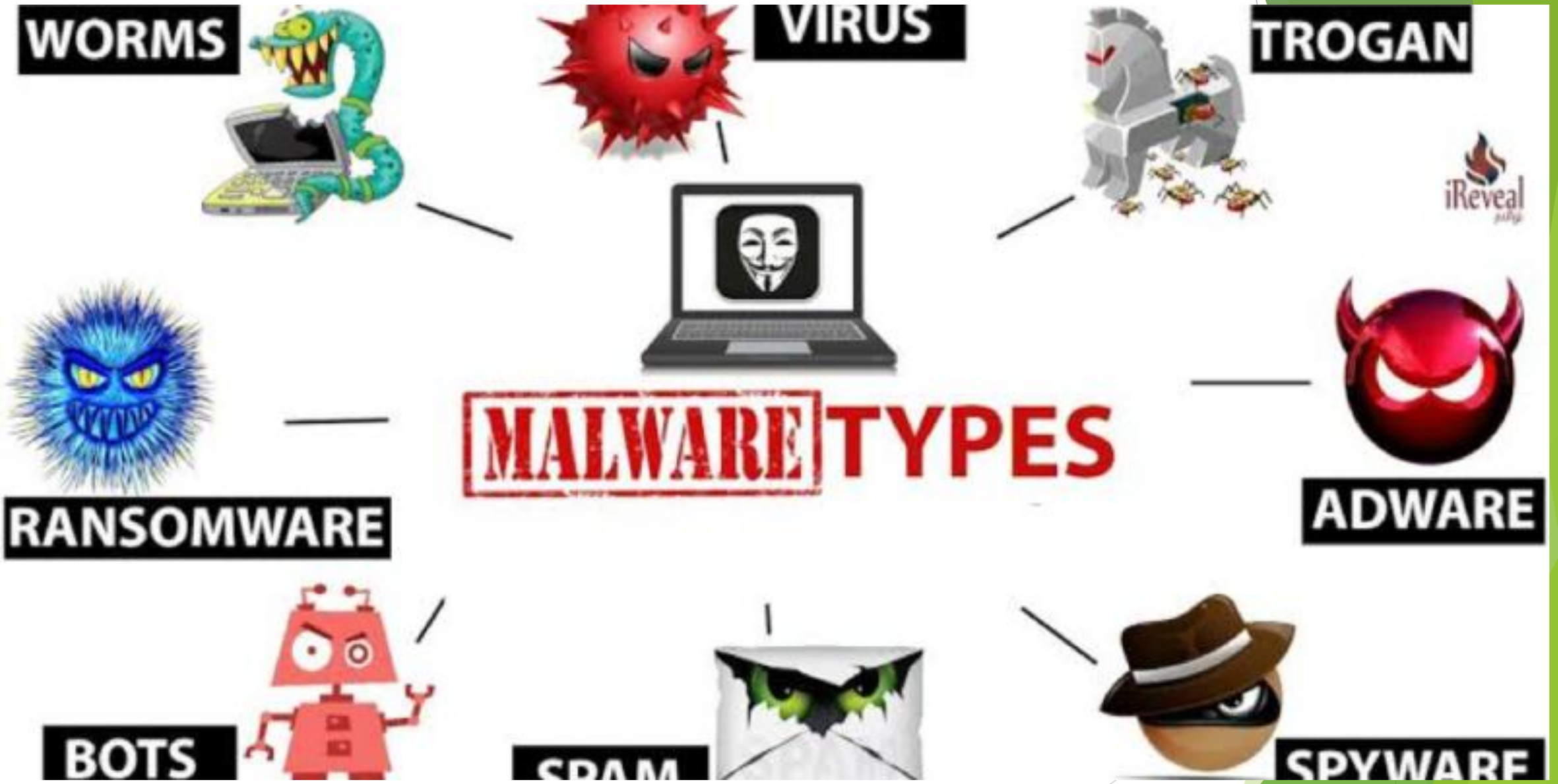
Malicious Software

Definisi Malicious Software

- Malware, atau malicious software, adalah program atau file apa pun yang berbahaya bagi pengguna komputer. Jenis malware dapat mencakup virus komputer, worm, trojan horse, dan spyware.
- Program jahat (Malware) ini dapat melakukan berbagai fungsi yang berbeda seperti mencuri, mengenkripsi atau menghapus data sensitif, mengubah atau membajak fungsi komputasi inti dan memantau aktivitas komputer pengguna tanpa izin mereka.

Cara Kerja Malware

Pembuat malware menggunakan berbagai cara fisik dan virtual untuk menyebarkan malware yang menginfeksi perangkat dan jaringan. Misalnya, program jahat dapat dikirimkan ke sistem dengan drive USB atau dapat menyebar melalui internet melalui download, yang secara otomatis mendownload program jahat ke sistem tanpa persetujuan atau pengetahuan pengguna.


WORMS
VIRUS
TROGAN
iReveal
MALWARE TYPES
RANSOMWARE
ADWARE
BOTS
SPAM
SPYWARE

Tipe-tipe Malware

- Virus adalah jenis malware yang paling umum yang dapat mengeksekusi sendiri dan menyebar dengan menginfeksi program atau file lain.
- Worm dapat mereplikasi diri sendiri tanpa program host dan biasanya menyebar tanpa ada interaksi manusia atau arahan dari pembuat malware.
- Trojan Horse dirancang untuk tampil sebagai program yang sah untuk mendapatkan akses ke suatu sistem. Setelah diaktifkan setelah instalasi, Trojans dapat menjalankan fungsi jahatnya.
- Spyware dibuat untuk mengumpulkan informasi dan data pada pengguna perangkat dan mengamati aktivitas mereka tanpa sepengetahuan mereka.

Tipe-tipe Malware

- Ransomware dirancang untuk menginfeksi sistem pengguna dan mengenkripsi data. Penjahat dunia maya kemudian menuntut pembayaran uang tebusan dari korban dengan imbalan mendekripsi data sistem.
- Rootkit dibuat untuk mendapatkan akses tingkat administrator ke sistem korban. Setelah terinstal, program ini memberikan root ancaman aktor atau akses istimewa ke sistem.
- Backdoor secara diam-diam membuat pintu belakang ke sistem yang terinfeksi yang memungkinkan pelaku ancaman mengaksesnya dari jarak jauh tanpa memberi tahu pengguna atau program keamanan sistem.

Tipe-tipe Malware

- Adware digunakan untuk melacak pengguna browser dan riwayat download dengan maksud untuk menampilkan iklan munculan atau spanduk yang memikat pengguna untuk melakukan pembelian. Misalnya, pengiklan dapat menggunakan cookie untuk melacak halaman web yang dikunjungi pengguna untuk iklan target yang lebih baik.
- Keyloggers, juga disebut monitor sistem, digunakan untuk melihat hampir semua yang dilakukan pengguna di komputer mereka. Ini termasuk email, halaman web yang terbuka, program, dan penekanan tombol pada keyboard.

Virus

- Orang cenderung menyebut malware sebagai virus, tetapi tidak demikian. Virus memodifikasi file host lain yang sah sedemikian rupa sehingga ketika mengeksekusi file di sistem korban, juga mengeksekusi virus. Saat ini, dengan berbagai jenis malware yang menginfeksi dunia cyber, virus komputer menjadi agak tidak biasa; mereka terdiri dari kurang dari 10% dari semua malware.
- Ingat, virus menginfeksi file lain, mereka adalah satu-satunya malware yang menginfeksi file lain dan karenanya sangat sulit untuk membersihkannya. sebagian besar waktu mereka menghapus atau mengkarantina file yang terinfeksi dan tidak menghilangkan virus itu sendiri.

Trojan (Remote Access Trojan)

- Trojan menyamar sebagai program yang sah. Namun, mereka mengandung instruksi jahat. Sebagian besar Trojan tiba melalui email atau menyebar dari situs web yang terinfeksi yang dikunjungi pengguna.
- Trojan hanya bekerja ketika korban mengeksekusi. Seorang pengguna mungkin menemukan pop up yang memberitahukan bahwa sistemnya terinfeksi. Munculan akan memerintahkannya untuk menjalankan program untuk membersihkan sistemnya padahal itu adalah Trojan.
- Trojan sangat umum, terutama karena Trojan mudah untuk ditulis. Selain itu, mereka mudah karena Trojan menyebar dengan menipu pengguna akhir untuk menjalankannya. Ini secara efektif menjadikan perangkat lunak keamanan tidak berguna.

Ransomware

- Ransomware, seperti namanya, menuntut tebusan untuk mengembalikan semuanya data yang diserang. Masalah utama dengan ransomware, yang akan menyebar sangat cepat di seluruh organisasi, jaringan, dan negara, adalah bahwa mereka mengenkripsi semua file dalam suatu sistem atau jaringan, menjadikannya tidak dapat diakses.
- Catatan tebusan muncul, menuntut pembayaran dalam cryptocurrency (uang digital), untuk mendekripsi file. Jika tebusan tidak dibayar, file yang dienkripsi akhirnya dapat dihancurkan dan karenanya ransomware harus dilihat sebagai salah satu bentuk malware yang paling menghancurkan.
- Kebanyakan ransomware adalah Trojan dan menyebar melalui rekayasa sosial.

Adware

- Adware tidak lain adalah upaya untuk mengekspos pengguna ke iklan yang tidak diinginkan dan berpotensi berbahaya.
- Iklan-iklan ini kemungkinan besar akhirnya menginfeksi perangkat pengguna. Ada program adware yang mengarahkan pengguna, selama pencarian browser, untuk mencari halaman web yang mirip dengan promosi produk lain. Menghapus adware lebih mudah cukup dengan menghapus aplikasi yang mengandung adware.

Spyware

- Spyware, seperti namanya, membantu hacker
  - memata-matai sistem dan penggunanya. Malware jenis ini dapat digunakan untuk key logging sehingga membantu hacker mendapatkan akses ke data pribadi dan kekayaan intelektual.

- Spyware juga digunakan oleh orang-orang yang ingin terus memeriksa aktivitas komputer orang-orang yang mereka kenal. Spyware, seperti adware, mudah dihapus.

Rootkit

- Rootkit adalah kumpulan perangkat lunak komputer, biasanya berbahaya, dirancang untuk memungkinkan akses ke komputer atau area perangkat lunaknya yang tidak diizinkan (misalnya, bagi pengguna yang tidak sah) dan sering kali menutupi keberadaannya atau keberadaan perangkat lunak lain.
- Rootkit istilah terdiri dari "root" (nama tradisional untuk akses administrator pada unix) dan kata "kit" (yang mengacu pada komponen perangkat lunak yang mengimplementasikan alat).

Cara mengatasi malware

- Install Anti-Virus/Malware Software dan selalu terupdate
- Lakukan scanning secara rutin
- Update sistem operasi
- Amankan kondisi jaringan
- Berhati-hati dalam mengeksekusi program yang tidak dikenal atau mengklik sebuah link
- Amankan data-data yang penting dengan melakukan backup secara berkala
- Jangan menggunakan jaringan Wifi yang tidak aman
- Menggunakan password yang kuat

Terimakasih