Nama : Usman
NIM : 22552021056
KELAS : Ti22A1

Jenis-Jenis Malware

Ransomware

Karakteristik

Malware yang mengenkripsi file korban dan meminta tebusan untuk mendapatkan kunci dekripsi.

Indicator of Compromise

- File terenkripsi dengan ekstensi aneh.
- Pesan tebusan (ransom note) muncul.
- Akses file penting ditolak.

Cara Melindungi

- Rutin backup data.
- Update software dan antivirus.
- Jangan klik link/email mencurigakan.

Trojan

Karakteristik

Malware yang menyamar sebagai software sah untuk menipu pengguna agar menginstalnya.

Indicator of Compromise

- Aktivitas sistem aneh (lambat, crash).
- Aplikasi tidak dikenal terinstal.
- Lalu lintas jaringan mencurigakan.

Cara Melindungi

- Hanya unduh software dari sumber terpercaya.
- Gunakan antivirus dengan deteksi real-time.
- Periksa dan batasi hak akses aplikasi.

Worm

Karakteristik

Malware yang mampu menggandakan dirinya dan menyebar ke komputer lain melalui jaringan.

Indicator of Compromise

- Kinerja jaringan lambat.
- Aktivitas aneh dalam log server.
- Peningkatan jumlah file/traffic tidak biasa.

Cara Melindungi

- Gunakan firewall.
- Update patch keamanan sistem.
- Segera matikan akses jaringan jika ada infeksi.

Spyware

Karakteristik

Malware yang diam-diam mengumpulkan informasi pengguna seperti password atau data pribadi.

Indicator of Compromise

- Iklan pop-up berlebihan.
- Browser redirect ke situs tidak dikenal.
- Penurunan kinerja sistem.

Cara Melindungi

- Gunakan anti-spyware.
- Hati-hati saat menginstal aplikasi gratis.
- Periksa pengaturan browser secara rutin.

Bloatware

Karakteristik

Aplikasi tidak perlu yang dibundel dalam perangkat, biasanya memperlambat sistem.

Indicator of Compromise

- Banyak aplikasi tidak berguna terinstal.
- Penyimpanan cepat penuh.
- Lambatnya startup sistem.

Cara Melindungi

- Hapus/uninstall aplikasi tidak penting.
- Pilih 'custom install' saat menginstal software.
- Gunakan aplikasi pihak ketiga untuk menghapus bloatware.

Virus

Karakteristik

Malware yang menempel pada file/program dan menyebar saat file tersebut dijalankan.

Indicator of Compromise

- File tiba-tiba hilang atau rusak.
- Performa sistem menurun drastis.
- Crash aplikasi atau sistem mendadak.

Cara Melindungi

- Gunakan antivirus terpercaya.
- Hindari membuka file mencurigakan.
- Backup file penting secara rutin.

Keylogger

Karakteristik

Malware yang merekam setiap penekanan tombol pada keyboard untuk mencuri informasi sensitif.

Indicator of Compromise

- Aktivitas keyboard terasa tidak normal.
- Kinerja komputer lambat tanpa alasan jelas.
- Deteksi program mencurigakan yang berjalan di background.

Cara Melindungi

- Gunakan antivirus dan anti-keylogger.
- Hindari mengunduh file dari sumber tidak terpercaya.
- Aktifkan autentikasi dua faktor (2FA).

Logic Bomb

Karakteristik

Kode berbahaya yang 'tidur' dalam sistem dan aktif berdasarkan kondisi tertentu (tanggal, tindakan tertentu).

Indicator of Compromise

- Perubahan file sistem tanpa sebab jelas.
- Aktivitas abnormal pada waktu tertentu.
- Kehilangan data tiba-tiba.

Cara Melindungi

- Audit kode secara berkala.
- Pantau perubahan file sistem.
- Gunakan sistem deteksi intrusi (IDS).

Rootkit

Karakteristik

Malware yang mendapatkan akses administrator ke sistem secara sembunyi-sembunyi.

Indicator of Compromise

- Antivirus dimatikan tanpa izin.
- Akses administratif tidak sah terdeteksi.
- Sistem menjadi tidak responsif terhadap perintah tertentu.

Cara Melindungi

- Gunakan rootkit scanner.
- Update sistem operasi dan software.
- Batasi hak akses administrator.