

**Apa Itu Ransomware, cara kerja, Jenis-Jenis, dan Cara Mencegahnya**

* **July 4, 2024**

Ransomware adalah salah satu *[cyber crime](https://www.dewaweb.com/blog/pengertian-dan-jenis-cyber-crime/" \o "cyber crime)* paling berbahaya di mana perangkat korban akan dikunci dan dienkripsi sehingga tidak bisa digunakan. Menurut [IBM X-Force Threat Intelligence Index](https://www.ibm.com/reports/threat-intelligence), ransomware terlibat dalam 20% dari seluruh serangan siber yang tercatat pada tahun 2023. Mengkhawatirkannya lagi, peretas hanya membutuhkan waktu kurang dari 4 hari untuk menyebarkan ransomware setelah mendapatkan akses ke jaringan target.

Menurut artikel [The Diplomat](https://thediplomat.com/2022/06/as-cyber-threats-grow-indonesias-data-protection-efforts-are-falling-short/), Indonesia mengalami serangan ransomware lebih banyak dibandingkan negara Asia Tenggara lainnya pada tahun 2021. Bahkan pada 20 Juni 2024 lalu, Pusat Data Nasional Sementara (PDNS) dilaporkan terserang ransomware. Alhasil, data dari [282](https://jateng.tribunnews.com/2024/06/29/data-diretas-hacker-sejak-20-juni-2024-belum-pulih-jokowi-minta-bpkp-audit-tata-kelola-pdn) instansi pemerintah yang tersimpan pada PDN terkunci dan tersandera.

## **Pengertian Ransomware**

*Ransomware*adalah jenis virus atau malware berbahaya yang digunakan untuk mengenkripsi data pengguna pada suatu perangkat komputer atau jaringan.

Aksi [pencurian data](https://www.linknet.id/article/apa-itu-data-breach-dan-cara-mencegahnya) ini umumnya bertujuan untuk memberikan keuntungan tertentu para pelaku di mana keuntungan tersebut berupa uang atau pembayaran lainnya.

*Ransomware*ini tentu menyebabkan kerugian cukup signifikan, baik secara finansial maupun pribadi. Selain itu, serangan *ransomware* juga dapat memengaruhi aktivitas individu dan operasional bisnis, seperti mengganggu sistem operasi dan layanan bisnis.

## **Cara Kerja Ransomware**

****

Secara umum, terdapat 7 langkah bagaimana ransomware akhirnya dapat mengacaukan sebuah sistem. Berikut penjelasannya.

**Infeksi:**Ransomware terunduh dan terinstal secara diam-diam di perangkat target.

**Eksekusi:**Malware memindai dan memetakan lokasi file target, termasuk penyimpanan lokal dan cloud.

**Enkripsi:** Ransomware melakukan pertukaran kunci dengan server kendali, mengenkripsi file yang ditemukan, dan mengunci akses data.

**Notifikasi:**Muncul pesan berisi informasi tebusan yang harus dibayar untuk mendapatkan kode dekripsi.

**Pembersihan:** Ransomware menghapus dirinya sendiri, menyisakan hanya file instruksi pembayaran.

**Pembayaran:** Korban diminta mengikuti instruksi pembayaran, biasanya melalui layanan TOR tersembunyi.

**Dekripsi:**Setelah pembayaran, korban menerima kode dekripsi untuk memulihkan akses. Namun, membayar tebusan tidak dianjurkan karena tidak ada jaminan pemulihan data.

## **Jenis Jenis Ransomware**

Menurut [Kaspersky](https://www.kaspersky.com/resource-center/threats/ransomware), ransomware terbagi menjadi dua jenis utama berdasarkan cara kerjanya, yaitu sebagai berikut:

### **1. Encrypting ransomware**

Encrypting ransomware, juga dikenal sebagai*crypto-ransomware,*yaitu jenis ransomware yang paling umum dan berbahaya. Malware ini bekerja dengan mengenkripsi file-file penting di perangkat korban, sehingga tidak dapat diakses tanpa kunci dekripsi. Setelah proses enkripsi selesai, penyerang akan menampilkan pesan yang meminta tebusan untuk mendapatkan kunci dekripsi.

Jenis ransomware ini sangat merusak karena dapat mengenkripsi berbagai jenis file, termasuk dokumen, foto, video, dan database. Beberapa varian encrypting ransomware yang terkenal termasuk WannaCry, CryptoWall, dan Locky. Tingkat risikonya sangat tinggi karena dapat menyebabkan kehilangan data permanen jika tidak ada [*backup*](https://www.dewaweb.com/blog/backup-data-pentingkah/) yang aman

### **2. Locker ransomware**

Locker ransomware bekerja dengan cara yang berbeda dari encrypting ransomware. Alih-alih mengenkripsi file, jenis ini mengunci akses pengguna ke seluruh sistem atau perangkat. Biasanya, locker ransomware menargetkan fungsi-fungsi sistem operasi, sehingga pengguna tidak dapat login atau menggunakan perangkat mereka secara normal.

Meskipun locker ransomware tidak merusak file secara langsung, dampaknya tetap signifikan karena menghentikan akses ke sistem dan data. Contoh locker ransomware termasuk Winlocker dan Reveton. Tingkat risikonya umumnya lebih rendah dibandingkan encrypting ransomware karena dalam beberapa kasus, ahli keamanan dapat memulihkan akses tanpa membayar tebusan.

## **Cara Mencegah Ransomware**

Untuk mencegah serangan ransomware, ada beberapa cara yang dapat kamu terapkan, berikut diantaranya.

**1. Perbarui sistem perangkat secara berkala**

Seperti yang sudah disebutkan sebelumnya, salah satu jenis *ransomware* bisa menyerang melalui sistem perangkat yang belum diperbarui. Pembaruan sistem perlu diperhatikan secara berkala karena pastinya ada peningkatan dari sistem keamanan yang digunakan atau yang lainnya.

### **2. Lakukan back-up rutin**

Salah satu teknik pencegahan yang cukup penting adalah melakukan *back-up* (pencadangan) data secara rutin. Proses ini dilakukan untuk mengantisipasi kehilangan data dengan menyalin atau menggandakan data pada media penyimpanan.

Sekarang ini, hampir seluruh perangkat dan media penyimpanan menyediakan fitur *back-up* otomatis. Jadi, Anda tidak perlu khawatir jika kelupaan untuk mencadangkan data.

### **3. Pakai jaringan internet yang aman**

Jika Anda sering menggunakan internet umum gratis, mungkin sekarang Anda perlu mempertimbangkannya kembali. Pasalnya, jaringan internet umum seringkali menjadi sasaran empuk para hacker untuk menanamkan virus pada perangkat Anda.

Hal ini disebabkan karena tidak semua internet umum menggunakan sistem keamanan andal sehingga memudahkan hacker untuk mengenkripsi data Anda.

Nah, sekarang Anda sudah lebih paham mengenai pengertian, cara kerja, hingga contoh kasusnya. Lakukan upaya pencegahan dengan mengikuti beberapa cara di atas atau bisa juga dengan menggunakan [jasa](https://www.linknet.id/product/penetration-test/improve-your-system-level)*[penetration testing](https://www.linknet.id/product/penetration-test/improve-your-system-level)*[dari Link Net](https://www.linknet.id/product/penetration-test/improve-your-system-level). Ketahui kelemahan sistem perangkat dengan *test*tersebut untuk mengambil langkah preventif yang tepat.

|  |
| --- |
| **REFERENSI :** Mengenal Apa Itu Ransomware, Jenis-Jenis, dan Cara Mencegahnya [*Mengenal Apa Itu Ransomware, Jenis-Jenis, dan Cara Mencegahnya - Dewaweb*](https://www.dewaweb.com/blog/apa-itu-ransomware/)  Apa itu Ransomware? Pengertian, Cara Kerja, dan Contoh  [*Apa itu Ransomware? Pengertian, Cara Kerja, dan Contoh Kasusnya - Link Net*](https://www.linknet.id/article/ransomware) |