

WASPADA

TOXICPANDA 2.0

ToxicPanda 2.0 merupakan malware Android yang mengincar aplikasi perbankan, e-wallet, pembayaran, dan cryptocurrency. Malware ini dapat menyalahgunakan berbagai izin akses pada perangkat untuk mengakses aktivitas dan informasi finansial pengguna.





Bagaimana malware masuk?

Waspada aplikasi dan tautan yang menyamar sebagai sesuatu yang terpercaya:

1. APK dari media sosial
2. Tautan phishing
3. Aplikasi bank palsu
4. Aplikasi keamanan palsu
5. Pembaruan system palsu



Kenali tanda mencurigakan

1. Wireless debugging tiba-tiba aktif
2. Muncul aplikasi yang tidak pernah kalian install
3. Aplikasi asing meminta banyak akses (galeri foto, kontak, kamera, dll)
4. Ponsel cepat panas atau baterai cepat habis
5. Muncul sistem update yang mencurigakan
6. Ada login atau transaksi yang tidak kalian lakukan

Langkah-Langkah mitigasi



1. Install aplikasi hanya dari sumber resmi
2. Jangan klik tautan mencurigakan
3. Periksa izin akses aplikasi secara berkala
4. Matikan wireless debugging jika tidak digunakan
5. Jangan bagikan PIN, OTP, atau password sembarangan



Jika terlanjur terinfeksi

1. Putuskan koneksi internet sementara
2. Hapus aplikasi yang mencurigakan
3. Ganti password dan PIN dari perangkat lain
4. Blokir akun atau kartu jika ada transaksi mencurigakan
5. Lakukan factory reset jika diperlukan

HOTLINE KEAMANAN INSIDEN SIBER

LINDUNGI RUANG SIBER KITA BERSAMA

Jika Anda mengalami atau menemukan insiden siber, segera laporkan melalui kanal resmi berikut agar dapat ditangani dengan cepat, tepat, dan terkoordinasi.



**BADAN SIBER
DAN SANDI
NEGARA**

✉ bantuan70@bssn.go.id

🌐 <https://www.bssn.go.id>



**PATROLI
SIBER**

✉ info@patrolisiber.id

🌐 <https://patrolisiber.id>



PEMERINTAH KOTA MATARAM
COMPUTER SECURITY INCIDENT RESPONSE TEAM

✉ csirt@mataramkota.go.id

🌐 <https://helpdesk.mataramkota.go.id>
(kategori Aduan Siber)

** Lampirkan bukti insiden (foto/screenshoot/log)
yang ditemukan*