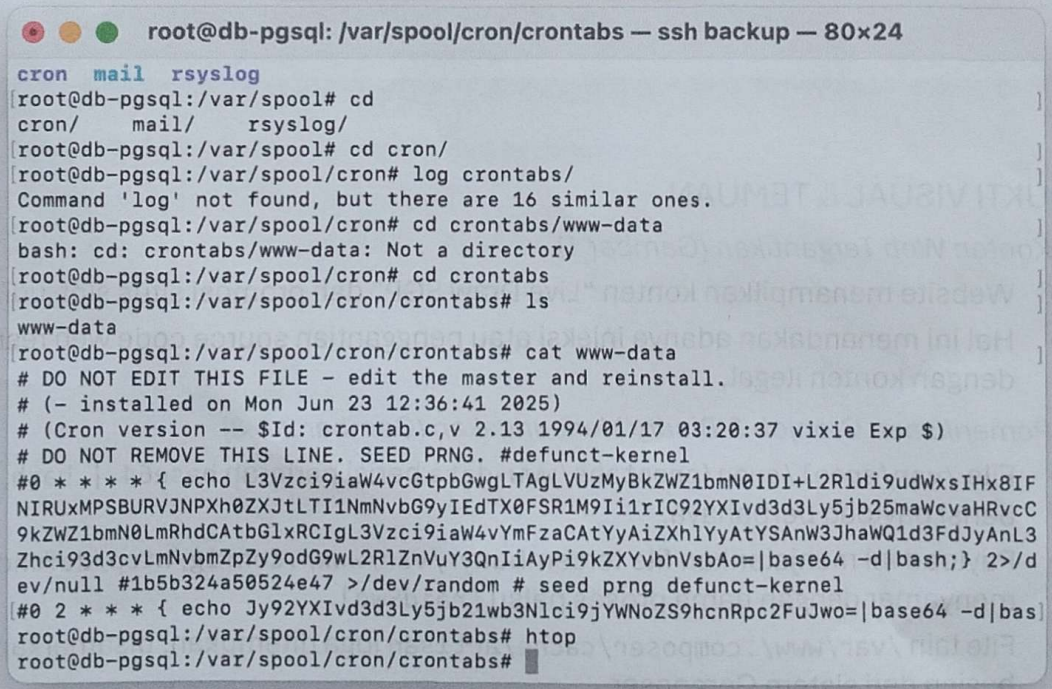
LAPORAN INSIDEN KEAMANAN SISTEM

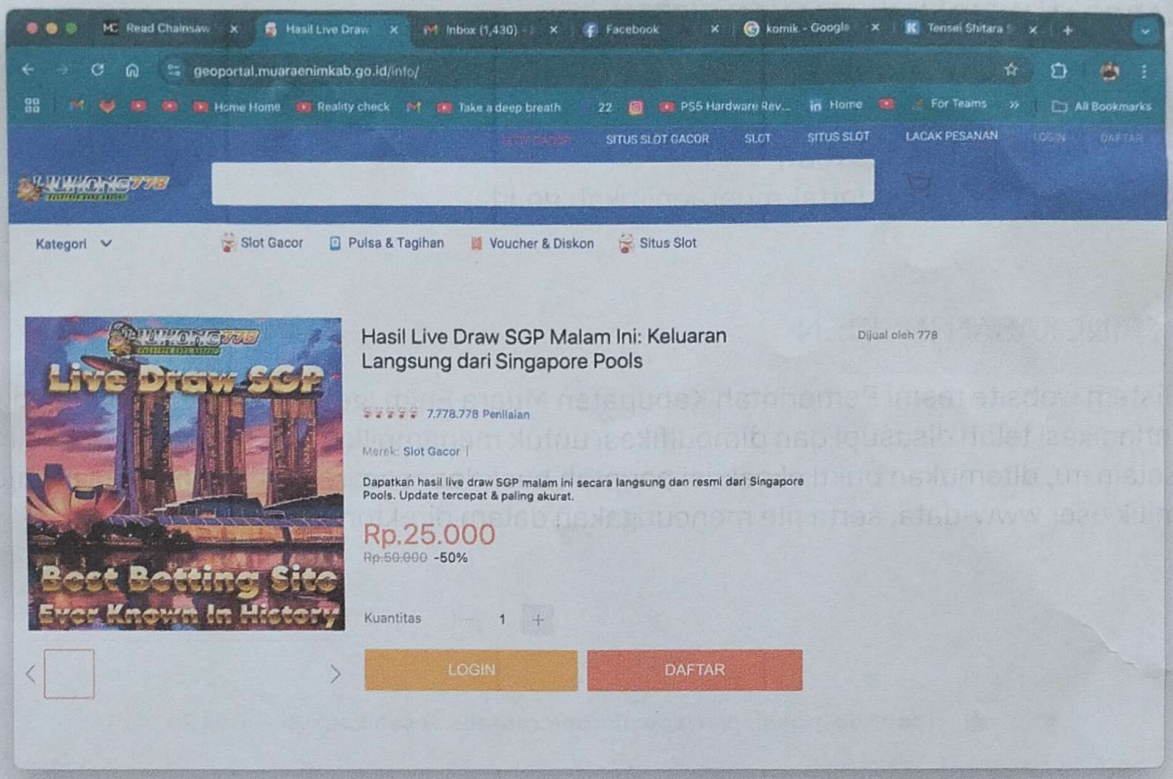
Nama Sistem: geoportal.muaraenimkab.go.id
Tanggal Deteksi: 3 Juli 2025
Server: db-pgsql (akses root)
Lokasi: /var/www/geoportal.muaraenimkab.go.id

---

1. RINGKASAN INSIDEN

Sistem website resmi Pemerintah Kabupaten Muara Enim (geoportal.muaraenimkab.go.id) terindikasi telah disusupi dan dimodifikasi untuk menampilkan konten perjudian online. Selain itu, ditemukan bukti eksekusi perintah backdoor secara periodik melalui cronjob milik user www-data, serta file mencurigakan dalam direktori sistem.





2. BUKTI VISUAL & TEMUAN

2.1. Konten Web Tergantikan (Gambar 1)

- Website menampilkan konten "Live Draw SGP" dan promosi situs slot judi.
- Hal ini menandakan adanya injeksi atau penggantian source code web resmi dengan konten ilegal.

2.2. Pemeriksaan Cronjob & Binary Mencurigakan (Gambar 2 & 3)

- File `/var/spool/cron/crontabs/www-data` berisi perintah `base64 | bash`, yang berisi payload berbahaya.
- Payload ini menjalankan file tersembunyi `/var/www/.config/htop/defunct` dan menyamar dengan nama proses palsu `[raid5wq]`.
- File lain `/var/www/.composer/cache/artisan` juga ditemukan, disamarkan seolah bagian dari sistem Composer.

2.3. Kegagalan Utilitas Standar

- Tools standar seperti `netstat`, `proftpd`, `crontab -e` tidak tersedia/berfungsi, menandakan kemungkinan sistem telah dimodifikasi oleh penyerang.

---

3. ANALISIS INSIDEN

- Penyerang berhasil memperoleh akses tulis pada sistem, kemungkinan melalui celah upload file atau injeksi web.
- Malware mempertahankan keberadaannya melalui cronjob user www-data.
- Teknik penyembunyian meliputi obfuscation base64, penggunaan nama proses palsu, dan peletakan binary di lokasi tidak wajar.

---

4. TINDAKAN YANG DIREKOMENDASIKAN

4.1. Isolasi

- Cabut koneksi internet dari server terindikasi.
- Backup penuh seluruh sistem untuk keperluan forensik.

4.2. Eliminasi Ancaman

- Hapus cronjob user www-data.
- Karantina file:
  - `/var/www/.config/htop/defunct`
  - `/var/www/.composer/cache/artisan`
- Hentikan proses aktif mencurigakan.

4.3. Audit & Recovery

- Cek integritas semua file sistem dan aplikasi.
- Re-deploy dari source yang bersih.
- Ganti seluruh kredensial (SSH, DB, dll).
- Tambahkan proteksi WAF, monitoring cron, dan file integrity checker (AIDE, etc).

---

5. STATUS DAN LANGKAH LANJUT

- Status: KRITIS (kompromi penuh web server).
- Rencana: Format ulang server dan deployment ulang sistem. Lanjutkan investigasi potensi penyusupan dari aplikasi.

Disusun oleh:
Bryan Wahyu
Diskominfo Muara Enim
Tanggal: 3 Juli 2025