SAFEnet



BOBOLNYA BENTENG MELAWAN JUDOL

Penyalahgunaan Situs Web Pemerintah untuk Iklan Judol di Indonesia

SAFEnet



BOBOLNYA BENTENG MELAWAN JUDOL

Penyalahgunaan Situs Web Pemerintah untuk Iklan Judol di Indonesia

Bobolnya Benteng Melawan Judol:
Penyalahgunaan Situs Web Pemerintah untuk Iklan Judol di Indonesia

Penulis
Andreas Takimai
Anton Muhajir
Abul Hasan Banimal
Ardy Wibisana

Editor
Anton Muhajir

Desain dan Tata Letak
Daeng Ipul

Januari 2026

Penerbit
Southeast Asia Freedom of Expression Network (SAFEnet)
Jl. Gita Sura III No. 55 Peguyangan Kaja
Denpasar, Bali 80123

Laporan ini menggunakan lisensi Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0). Anda bebas untuk untuk mendistribusikan, mencampur ulang, mengadaptasi, dan membuat materi dalam media atau format apa pun hanya untuk tujuan nonkomersial, dan hanya selama atribusi diberikan kepada pencipta. Informasi lebih lanjut di https://creativecommons.org/licenses/by-nc/4.0/

Daftar Isi

Ringkasan 1
Pendahuluan 3
Latar Belakang 3
Batasan 6
Pembahasan 8
- Kata Kunci 8
- Teknis Promosi 9
- TOTO 9
- Slot 9
- Bet 10
- 14D 10
- Angka Khas 10
- Slang 10
- Hoki 11
- Olahraga 11
- Ikon Mitologi 11
- Jenama Lokal 11
- Pengumpulan Domain 12
- Relevansi Domain .go.id 13
- Ketidaksesuaian Aturan Penulisan Domain 17
- Indikasi Injeksi 19
- Kata Kunci yang Digunakan 21
- Metode Penyebaran 25
- Pemindaian Sucuri 27
- Pengecekan Pemblokiran 28
- Mekanisme Penanganan 30

Penutup 34
Kesimpulan 34
Rekomendasi 35
Glosarium 37



Ringkasan



Di tengah gencarnya perang terhadap judi *online* (selanjutnya disebut judol), serangan terhadap situs web pemerintah justru menjadi situasi yang seolah terlupakan. Riset SAFEnet menemukan bahwa situs web dengan ekstensi .go.id, sebagai simbol dari kedaulatan siber negeri ini, justru termasuk yang rentan mengalami serangan dalam bentuk penyisipan iklan dan tautan bermuatan judol.

Serangan dalam bentuk penyisipan tautan judol tersebut telah menjangkau berbagai sektor pemerintahan, mulai dari lembaga peradilan, dinas pendidikan, hingga pengawasan pemilu di tingkat daerah. Setelah melakukan pencarian terhadap 160.824 subdomain yang dikelola pemerintah, ditemukan 3.625 domain yang terindikasi memuat tautan ke situs judol.

Kasus paling berat terjadi pada akta.pa-masamba.go.id dengan 2.232 tautan judol, diikuti dindikbud.demakkab.go.id (1.427 tautan), dan dinperkim. demakkab.go.id (1.415) tautan. Situs web lain menunjukkan pola penyebaran konten judi daring di subdomain instansi pemerintahan berlangsung melalui dua jalur utama, yakni kata kunci *(keyword seeding)* dan judul berita palsu *(narrative injection)*. Kedua metode ini saling melengkapi: kata kunci berfungsi untuk menembus sistem indeks mesin pencari secara teknis, sementara judul berita digunakan untuk menarik perhatian pengguna manusia melalui narasi lokal yang seolah-olah benar atau sah.

Masalah utama maraknya serangan injeksi judol pada situs web pemerintah yang berakar pada tiga aspek, yaitu tata kelola, sumber daya manusia, dan teknologi. Tidak adanya kebijakan di tingkat lokal dan pusat membuat pemantauan dan penanganan terhadap serangan siber tautan judol ini tidak berjalan dengan baik. Bahkan di tingkat pusat pun masih sering terjadi lempar tanggung jawab antara Komdigi dan BSSN.

Dari sisi sumber daya manusia, terbatasnya kapasitas sumber daya dari sisi kualitas dan kuantitas masih terus menjadi tantangan. Jumlah staf keamanan siber masih amat terbatas dibandingkan banyaknya tanggung jawab yang harus mereka lakukan. Juga karena metode serangan siber yang terus berkembang tak diiringi peningkatan kapasitas sumber daya manusia.

Terakhir, dari sisi teknologi, penggunaan CMS populer Wordpress menjadi salah satu sumber kerentanan selain juga PHP dan sertifikat SSL yang kedaluwarsa atau salah pengaturan.

Untuk menjawab tantangan tersebut, pemerintah perlu membuat kebijakan tegas bagi instansi pemerintah agar lebih mengamankan situs-situs web mereka dari serangan judol, termasuk mekanisme koordinasi yang lebih jelas dalam penanganan insiden. Peningkatan kapasitas sumber daya manusia melalui pengetahuan dan keterampilan, serta penambahan jumlah staf menjadi hal mendesak untuk menjawab kurangnya kapasitas SDM. Terakhir, audit keamanan secara berkala juga penting agar teknologi yang digunakan bisa segera diperbaiki atau ditingkatkan ketika terdapat celah yang menyumbang terhadap kerentanan.

Pendahuluan



Latar Belakang

Pemerintah Indonesia sedang gencar-gencarnya melakukan perang terhadap judi *online* (judol). Selain menggunakan regulasi yang sebelumnya sudah ada, seperti Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 303 dan Pasal 303 *bis* serta UU Informasi dan Transaksi Elektronik (UU ITE), Pemerintah juga menerbitkan Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik (PSE).

Sebagai pelaksana teknis pemberantasan judol, Pemerintah Indonesia membentuk Satuan Tugas Pemberantasan Perjudian Daring (Satgas Judol) melalui Keputusan Presiden (Keppres) Nomor 21 Tahun 2024. Satgas ini bertugas untuk memberantas kegiatan judol dengan melibatkan berbagai lembaga negara, termasuk Kominfo (saat ini menjadi Kementerian Komunikasi dan Digital atau Komdigi), Kepolisian Republik Indonesia (Polri), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), dan lain-lain.

Namun, gencarnya perang terhadap judol tersebut belum diiringi pula dengan penguatan terhadap lembaga pemerintah itu sendiri, yaitu situs web yang mereka kelola. Padahal, pemerintah seharusnya mampu menjadi benteng tangguh dalam perang melawan judol tersebut.

Selama lima tahun terakhir, iklan atau tautan ke situs judol di situs web resmi lembaga pemerintah Indonesia (misalnya .go.id) semakin marak. Iklan atau tautan tersebut muncul terutama ketika pengguna mencari kata kunci tertentu. Kata-kata seperti slot, gacor, cuan, togel, dan semacamnya ternyata mudah ditemukan di situs web dengan ekstensi .go.id, baik itu di tingkat kabupaten, provinsi, maupun lembaga negara lain.

Fenomena ini menunjukkan adanya celah keamanan, pengelolaan yang lemah, atau bahkan kemungkinan pembajakan akses administratif terhadap situs-situs publik yang seharusnya aman dan terpercaya. Pelaku serangan dalam bentuk penyisipan iklan atau tautan bisa melakukannya memanfaatkan celah keamanan tersebut, baik dari sisi teknis maupun pengelolanya.

Penyalahgunaan ini tidak hanya merusak reputasi lembaga terkait, tetapi juga menurunkan kepercayaan publik terhadap institusi negara dan

menimbulkan risiko hukum dan keamanan digital. Situs web pemerintah seharusnya memiliki kredibilitas dari sisi keandalan (*reliability*) dan keamanan (*security*), termasuk aman dari penyisipan tautan judol ke dalam situs web mereka.

Namun, meskipun serangan dalam bentuk penyisipan iklan atau tautan tersebut makin marak, informasi tentang metode dan dampak serangan ini masih sangat terbatas. Atau bahkan belum sama sekali. Oleh karena itu, SAFEnet melakukan riset ini untuk mengidentifikasi skala penyalahgunaan ini secara sistematis dan mendalam.

Melalui riset ini, SAFEnet berharap bisa menjawab tiga pertanyaan. Pertama, mengidentifikasi situs-situs web pemerintah Indonesia yang menunjukkan indikasi penyalahgunaan untuk iklan atau tautan ke situs judol. Kedua, mengklasifikasikan jenis penyalahgunaan yang terjadi. Apakah dalam bentuk injeksi iklan, *redirect*, pembajakan sistem penamaan domain (DNS), atau bentuk lainnya. Ketiga, menilai tingkat keamanan teknis situs web yang terdampak. Dari tiga pertanyaan tersebut, kami berharap bisa memberikan rekomendasi mitigasi bagi pengelola situs pemerintah meskipun masih bersifat umum.

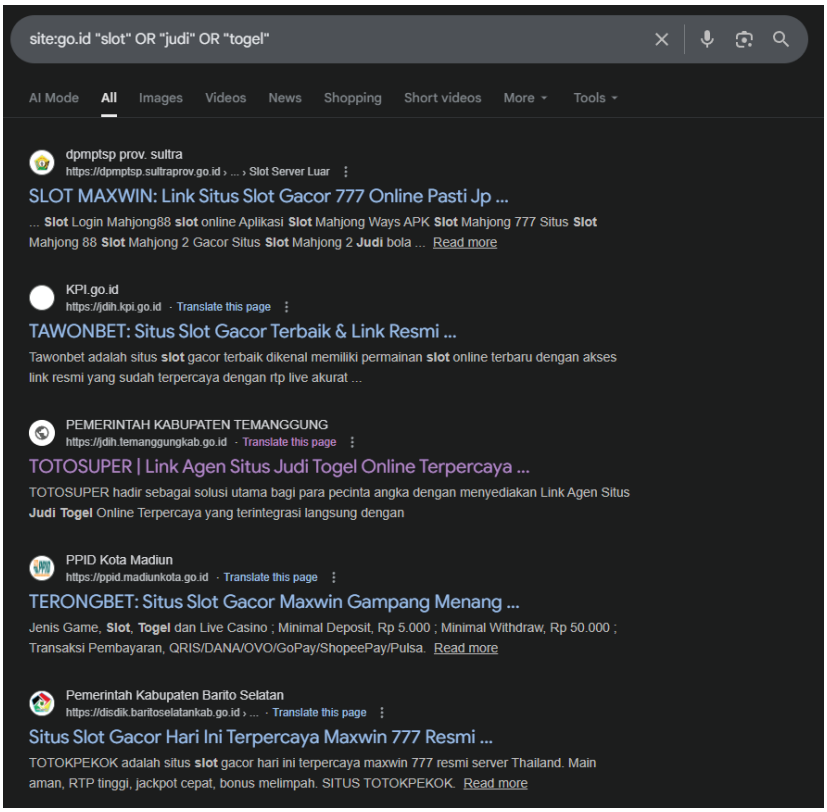
Metodologi

Untuk menjawab pertanyaan-pertanyaan tersebut, kami menggunakan sejumlah pendekatan dan alat bantu sebagai bagian dari metodologi riset kami.

Ada empat pendekatan dalam riset ini. Pertama, melalui pengumpulan sumber data domain tingkat atas kode negara atau *country-code top level domain* (ccTLD) melalui *open source intelligence (OSINT).* Kedua, penggunaan mesin pencari, *cache*, dan alat analisis metadata untuk mencari kata kunci judi dan situs dengan kategori domain atau *top-level domain* (TLD) go.id. Ketiga, pemindaian terbatas menggunakan peranti (*tools*), seperti wget, curl, dan grep untuk mendeteksi konten mencurigakan. Terakhir, kami melakukan pemeriksaan lanjutan atau verifikasi secara manual terhadap situs yang terindikasi.

Untuk menerapkan pendekatan tersebut, kami menggunakan setidaknya tiga alat bantu yaitu Google Dork: site:go.id “slot” OR “judi” OR “togel”; tools seperti cURL, Wget, Python (BeautifulSoup, requests); serta penggunaan *inspect element* untuk verifikasi manual.

Google Dorks biasanya digunakan sebagai tahap awal pencarian dan pemetaan informasi (OSINT) untuk menemukan halaman web tertentu



Gambar 1: Hasil pencarian dengan Google Dorks

yang mengandung kata kunci pada domain tertentu. Dengan perintah seperti site:go.id "slot" OR "judi" OR "togel", Google Dorks membantu mengidentifikasi indikasi awal adanya konten judi, *spam SEO*, atau penyalahgunaan domain go.id dapat diakses publik. Teknik ini dipakai untuk pengumpulan indikasi sebelum dilakukan verifikasi lanjutan.

Tools lain seperti cURL, Wget, Python (*requests* dan *BeautifulSoup*), serta *Inspect Element* digunakan pada tahap verifikasi dan analisis lanjutan. cURL dan Wget membantu mengambil konten halaman secara langsung untuk memastikan apakah isi yang terindeks Google benar-benar ada dan melihat *respons server*. Python dengan *requests* dan *BeautifulSoup* dipakai untuk analisis yang lebih terstruktur dan otomatis, misalnya mengumpulkan banyak halaman, mengekstrak teks atau metadata, dan mengelompokkan temuan. Adapun *inspect element* digunakan untuk verifikasi manual di peramban, seperti memeriksa konten tersembunyi, injeksi web judol. Keseluruhan *tools* ini dipakai untuk analisis konten publik, audit, dan dokumentasi temuan.

Sebagai ruang untuk diskusi, terutama dengan pemerintah dan para ahli, kami juga melaksanakan diskusi secara daring pada 7 November 2025. Diskusi menghadirkan narasumber dari tiga kalangan, yaitu Kementerian Komunikasi dan Digital (Komdigi), akademisi Pusat Ilmu Komputer Universitas Indonesia (Pusilkom UI), dan komunitas keamanan siber. Dalam diskusi ini, tim riset SAFEnet juga menyampaikan temuan awal sehingga bisa menjadi forum menanggapi temuan tersebut.

Batasan

Sebagai transparansi, riset ini juga menerapkan sejumlah batasan. Pertama, riset hanya fokus pada penyalahgunaan domain .go.id untuk promosi judol. Tim riset hanya menganalisis konten pada halaman yang memuat indikasi promosi judol. Pendekatan tim riset bersifat non-intrusif, tanpa melakukan pengujian lebih lanjut, termasuk uji penetrasi (*pentest*), penggantian tampilan (*defacement*), pembocoran data (*data breach*) atau penolakan layanan (DDoS). Tim riset juga tidak menyentuh data sensitif, seperti pangkalan data pengguna, login admin, atau dokumen internal.

Oleh karena itu, temuan-temuan dalam riset ini hanya bersifat indikasi, bukan bukti hukum. Kami juga tidak menilai sejauh mana efektivitas pemblokiran nasional, tetapi hanya meninjau aksesibilitas situs judol pada domain .go.id.

Terakhir, pemantauan dan pemindaian ini kami lakukan hanya selama tiga bulan pada Agustus hingga Oktober 2025. Oleh karena itu, situasinya mungkin akan berbeda di waktu lain pula. Karena alasan inilah maka sangat penting untuk ada riset lanjutan agar semakin banyak informasi terkait kerentanan situs web pemerintah dari serangan judol ini.

Pembahasan

Secara garis besar, ada empat tahap yang kami lakukan untuk menemukan situs-situs web pemerintah yang menjadi korban serangan penyisipan iklan dan tautan situs web judol, yaitu pencarian kata kunci, identifikasi situs-situs web yang diserang, analisis lanjutan, serta verifikasi manual. Setiap tahapan akan dijelaskan lebih lanjut, termasuk tambahan informasi jika diperlukan.

Kata Kunci

Pencarian kata kunci dilakukan menggunakan mesin pencari seperti Google. Setelah, menemukan dari berbagai sumber, hasil pencarian dikompilasikan menjadi satu dan terkumpul sejumlah 1.290 kata. Dalam eksplorasi mendalam terhadap kumpulan kata kunci yang ditemukan dari berbagai sumber, kami menemukan sebelas klaster utama yang membentuk pola linguistik dan operasional konsisten di ekosistem situs judol. Setiap klaster tidak hanya berfungsi sebagai penanda, tetapi juga mencerminkan strategi semantik yang disengaja untuk menarik pengguna, menghindari deteksi otomatis, dan membangun legitimasi palsu.

Tabel 1 Klaster Penanda Judol

Klaster	Contoh
RTP (Teknis–Promo)	rtp, rtplive, rtpirit4d, rtpindobit, rtphoki
TOTO / TOGEL / LOTTO (Angka 4D)	toto, togel, toggel, lotto, pangerantoto
SLOT (Permainan Utama)	slot, sukaslot, hokislot, sniperslot
BET / WIN / VIP (Taruhan dan Insentif)	bet, win, vip, jackpot, spingratis
4D (Ciri Togel Indonesia)	vip4d, halo4d, garuda4d
Angka Khas (Numerik Branding)	88, 77, 138, 303, 365
Slang / Promosi (Bahasa Emosional)	gacor, maxwin, cuan, hadiah
HOKI / JP (Keberuntungan Lokal)	hoki, hokislot, kakekjp
QQ / BOLA / SPORT (Taruhan Olahraga dan Poker)	qqslot, idnsport, operabola
Brand / Ikon Mitologi (Visual Imitation)	zeus, kraken, athena, medusa, istana, vegas
Merek Lokal / Nasional	nusabet, jawaraslot, kampungtoto, warunggol

Berikut penjelasan lebih detail tentang karakteristik, contoh-contoh spesifik, serta implikasi yang muncul dari pola-pola tersebut.

Teknis Promosi

Klaster pertama yang menonjol adalah RTP, yang sering dikategorikan sebagai istilah teknis-promosi. Kata-kata kunci seperti "rtp", "rtplive", "rtpirit4d", "rtpindobit", dan "rtphoki" berasal dari konsep *"Return To Player"* dalam permainan mesin slot, yang memberikan kesan ilmiah atau teknis kepada pengguna. Pola ini berperan sebagai *"teknik jebakan"*, sebuah taktik untuk membangun kepercayaan palsu dengan menggunakan terminologi yang terdengar profesional, seolah-olah situs tersebut didasarkan pada data atau algoritma akurat. Hal ini sering kali digunakan untuk menipu pengguna yang mencari informasi teknis tentang peluang kemenangan, sehingga meningkatkan interaksi dengan domain yang sebenarnya berisiko tinggi.

TOTO

Klaster TOTO, TOGEL, dan LOTTO menunjukkan fokus pada aktivitas taruhan angka, khususnya dalam format 4D. Contoh-contoh seperti "toto", "togel", "toggel", "lotto", dan "pangerantoto" mengindikasikan variasi ejaan yang sengaja dibuat untuk menghindari filter otomatis, sebuah teknik yang dikenal sebagai *"linguistic obfuscation"* atau pengaburan melalui bahasa. Temuan ini menunjukkan bahwa klaster ini kuat terkait dengan pasar Asia Tenggara.[1] Dengan variasi seperti "toggel", operator domain mencoba mengelabui sistem deteksi sederhana, sambil tetap menjaga daya tarik bagi audiens yang familiar dengan istilah-istilah tersebut.

Slot

Klaster slot muncul sebagai inti dari banyak domain berisiko. Contohnya, "slot", "sukaslot", "hokislot", dan "sniperslot". Kata kunci ini merupakan indikator leksikal utama yang paling sering muncul dalam analisis, berfungsi sebagai fondasi untuk kata kunci yang dapat digunakan dalam deteksi domain mencurigakan. Dalam temuan, klaster ini menekankan bagaimana kata "slot" menjadi pusat ekosistem perjudian daring, sering kali dikombinasikan dengan elemen lain untuk menciptakan nama domain yang menarik.

---

1 *https://www.cnnindonesia.com/internasional/20240620141343-106-1111940/negara-mana-tampung-bandar-judi-online-terbesar-di-asia-tenggara*

Bet

Klaster BET, WIN, dan VIP membawa nuansa taruhan dan insentif, dengan contoh seperti "bet", "win", "vip", "jackpot", dan "spingratis". Temuan ini mengungkapkan bagaimana kata-kata ini digunakan untuk membangun narasi kemenangan dan keuntungan. Sering kali dalam bentuk "clickbait incentive" yang dirancang untuk memicu emosi pengguna. Dalam konteks *phishing* atau *malvertising*, klaster ini sangat efektif karena menjanjikan hadiah atau keuntungan instan, sehingga mendorong klik dan interaksi yang berisiko. Analisis lebih lanjut menunjukkan bahwa pola ini sering muncul di domain yang terhubung dengan kampanye *spam* iklan, di mana legitimasi dibangun melalui janji-janji yang tidak realistis.

14D

Klaster 4D, sebagai ciri khas togel Indonesia, ditandai oleh contoh seperti "vip4d", "halo4d", dan "garuda4d". Kata kunci ini berfungsi sebagai penanda geografis, menunjukkan operasi jaringan lokal yang kuat di Indonesia. Temuan ini berguna untuk *"geo-tagging"* dalam analisis regional, di mana "4d" menjadi simbol budaya perjudian angka yang spesifik. Dengan mengintegrasikan angka ini ke dalam nama domain, operator menciptakan identitas yang familiar bagi audiens lokal, sambil memperluas jangkauan ke pasar domestik lebih luas.

Angka Khas

Klaster angka khas, seperti "88", "77", "138", "303", dan "365", mewakili *branding* numerik yang didasarkan pada simbol keberuntungan Asia. Temuan ini menunjukkan bagaimana angka-angka ini sering digunakan dalam algoritma pembuatan domain massal, seperti *Domain Generation Algorithms (DGA)*, untuk menghasilkan variasi domain yang mirip, tapi unik. Dalam narasi ini, angka seperti "88" – yang dianggap membawa keberuntungan ganda – menjadi elemen kunci dalam strategi *branding*, memungkinkan produksi domain dalam skala besar tanpa terdeteksi mudah oleh sistem keamanan.

Slang

Klaster ragam bahasa tidak resmi (slang) dan promosi, dengan contoh seperti "gacor", "maxwin", "cuan", dan "hadiah", mencerminkan bahasa emosional yang dirancang untuk menarik perhatian. Kata-kata ini berfungsi sebagai "social engineering lexical indicators", memanfaatkan emosi seperti

keserakahan atau ketakutan untuk meningkatkan potensi klik. Temuan analisis menekankan bahwa klaster ini sering muncul dalam injeksi SEO dan iklan *spam*, di mana bahasa sehari-hari digunakan untuk membuat konten terasa lebih personal dan menarik, sehingga memperbesar risiko interaksi dengan domain berbahaya.

Hoki

Klaster HOKI dan JP, seperti "hoki", "hokislot", dan "kakekjp", membawa konteks budaya Indonesia-Tionghoa yang kuat. Temuan ini menunjukkan segmentasi audiens lokal, di mana "hoki" – yang berarti keberuntungan – digunakan untuk menarik pengguna yang percaya pada konsep-konsep tradisional. Dalam narasi, klaster ini mengungkapkan bagaimana operator domain menyesuaikan bahasa dengan orientasi pasar lokal, menciptakan koneksi budaya yang lebih dalam dan meningkatkan loyalitas audiens.

Olahraga

Klaster QQ, BOLA, dan SPORT, dengan contoh seperti "qqslot", "idnsport", dan "operabola", menandai ekspansi perjudian ke sektor olahraga dan poker. Temuan ini mengindikasikan afiliasi dengan jaringan besar seperti IDN Network atau Asia Gaming, di mana taruhan olahraga menjadi ekstensi dari permainan kartu. Analisis lebih lanjut menunjukkan bahwa klaster ini mencerminkan diversifikasi operasi, memungkinkan operator untuk menjangkau audiens lebih luas di luar mesin slot tradisional.

Ikon Mitologi

Klaster brand dan ikon mitologi, seperti "zeus", "kraken", "athena", "medusa", "istana", dan "vegas", menggunakan elemen visual dan mitologis untuk meniru legitimasi merek internasional. Temuan ini menyoroti "brand spoofing", di mana nama-nama ikonik digunakan untuk membangun kepercayaan palsu. Klaster ini berguna untuk mendeteksi perilaku ancaman yang melibatkan imitasi visual, seperti situs yang menyerupai kasino terkenal untuk menipu pengguna.

Jenama Lokal

Klaster jenama atau merek lokal dan nasional, seperti "nusabet", "jawaraslot", "kampungtoto", dan "warunggol", menunjukkan fokus pada segmentasi pasar Indonesia. Temuan ini mengungkapkan bagaimana nama-nama yang terdengar familiar digunakan untuk melacak rantai distribusi konten ilegal

di jaringan domestik. Dalam konteks ini, klaster ini menjadi alat untuk memahami dinamika pasar lokal, di mana operator memanfaatkan identitas nasional untuk memperkuat daya tarik dan menghindari pengawasan internasional.

Secara keseluruhan, temuan kata kunci ini menggambarkan ekosistem yang kompleks dan strategis. Setiap klaster saling terkait untuk membentuk pola yang efektif dalam menarik dan menipu pengguna. Dengan memahami detail ini, analisis dapat digunakan untuk pengembangan alat deteksi yang lebih canggih.

Pengumpulan Domain

Tahapan kedua setelah menemukan apa saja kata kunci yang digunakan untuk memancing pengguna internet agar terjebak dengan judol adalah mengumpulkan lokasi-lokasi di mana kata kunci tersebut diselipkan. Salah satunya dengan terlebih dulu melihat struktur penamaan domain di Indonesia, termasuk sejarahnya.

Berdasarkan catatan resmi Pengelola Nama Domain Internet Indonesia (PANDI), sejarah domain internet Indonesia bermula pada tahun 1993, ketika kode negara .id didaftarkan oleh Internet Assigned Numbers Authority (IANA) kepada Indonesia. Pada masa awal, pengelolaan domain .id dilakukan secara sukarela oleh komunitas teknis dan akademik, sebelum dibentuknya lembaga resmi nasional.[2]

PANDI berdiri pada 1 September 2006 sebagai badan hukum independen yang mewakili komunitas internet, pemerintah, dan industri, dengan tujuan mengelola nama domain Indonesia secara profesional. Pengelolaan administrasi domain .id secara resmi diserahkan kepada PANDI melalui Berita Acara Penugasan Administrasi Domain .id No. BA-343/DJAT/MKOMINFO/6/2007 pada 29 Juni 2007. Setelah itu, PANDI menjalankan fungsi registri nasional untuk domain .id di bawah koordinasi Kominfo pada saat itu.

Dalam struktur pengelolaan yang ditetapkan PANDI, domain .id dibagi ke dalam beberapa domain tingkat kedua atau *second-level domain* (SLD) untuk membedakan fungsi dan jenis penggunanya. Di antaranya adalah: .co.id untuk badan usaha dan perusahaan komersial, .or.id untuk organisasi non-profit, .ac.id untuk perguruan tinggi, .sch.id untuk sekolah, .mil.id untuk institusi militer, dan .go.id untuk lembaga pemerintahan. Domain .go.id berasal dari kata "*government*" dan ditetapkan sebagai domain eksklusif yang hanya dapat digunakan oleh instansi pemerintah.

---

2 *https://pandi.id/en/blog/sejarah-pengelola-nama-domain-internet-indonesia-pandi-sebagai-registri-id*

Pendaftaran domain .go.id diatur dengan ketat sesuai kebijakan PANDI dan Kominfo. Persyaratannya adalah surat keputusan pembentukan lembaga, surat permohonan resmi dengan kop instansi, identitas pejabat penanggung jawab, serta bukti alamat dan struktur organisasi. Kebijakan tersebut untuk memastikan bahwa domain .go.id berfungsi sebagai identitas digital resmi pemerintah Indonesia, dan setiap entitas yang menggunakannya merupakan lembaga yang sah secara hukum.

Menurut catatan PANDI, ketika lembaga ini mulai beroperasi, terdapat sembilan SLD yang dikelola, termasuk go.id. Kini, PANDI mengelola lebih dari sepuluh kategori domain di bawah .id, di antaranya go.id, co.id, or.id, ac.id, sch.id, mil.id, net.id, web.id, desa.id, dan my.id. Domain .go.id tetap memiliki posisi strategis karena menjadi simbol legitimasi dan otoritas negara di internet, serta mewakili tata kelola digital pemerintahan Indonesia di tingkat nasional maupun daerah.

Dengan demikian, berdasarkan catatan resmi PANDI, perjalanan domain .id, khususnya .go.id, menunjukkan proses institusionalisasi pengelolaan identitas digital nasional. Sejak pengalihan pengelolaan kepada PANDI pada tahun 2007, domain .go.id berperan sebagai wajah digital pemerintah Indonesia, dan menjadi bagian dari infrastruktur resmi yang mendukung keterbukaan informasi serta pelayanan publik berbasis elektronik di Indonesia.

Relevansi Domain .go.id

Karena domain .go.id merepresentasikan lembaga publik di seluruh tingkatan pemerintahan, mulai dari kementerian, lembaga negara, hingga pemerintah daerah, maka riset ini berfokus pada domain .go.id. Fokus tersebut dipilih karena .go.id tidak hanya berfungsi sebagai alamat situs, tetapi juga sebagai identitas digital resmi negara yang menunjukkan keberadaan dan kinerja lembaga pemerintahan di ruang siber. Setiap domain .go.id mewakili entitas publik yang memiliki otoritas administratif, legalitas kelembagaan, serta tanggung jawab terhadap layanan dan informasi yang disediakan secara daring. Oleh karena itu, analisis terhadap .go.id memberikan gambaran paling representatif tentang arsitektur digital pemerintahan Indonesia, baik dari segi struktur birokrasi, infrastruktur teknis, maupun kebijakan pengelolaan data dan keamanan.

Pemilihan fokus pada domain .go.id juga didasarkan pada karakteristiknya yang terverifikasi dan terstandar secara nasional di bawah pengawasan PANDI dan Komdigi. Dengan legitimasi tersebut, penelitian ini dapat

mengandalkan domain .go.id sebagai ruang observasi yang sah dan terpercaya untuk memahami perkembangan tata kelola digital, pola komunikasi lembaga publik, serta dinamika keamanan informasi di ranah pemerintahan Indonesia.

Setelah berbagai penelusuran di peramban, ditemukan 160.824 subdomain dan domain utama dari berbagai sumber. Domain tersebut dilakukan pengujian keaktifan secara otomatis. Dari hasil pengujian ditemukan bahwa hanya sebagian kecil yang masih aktif dan memberikan respons normal, sementara sebagian besar sudah tidak dapat diakses sama sekali. Sebanyak 35.089 domain terdeteksi dengan status 200 (berhasil), yang berarti peladen masih berjalan dan menanggapi permintaan dengan benar. Namun, jumlah ini hanya sekitar 21,8% dari total keseluruhan, menunjukkan bahwa sebagian besar domain yang diuji sudah tidak lagi beroperasi secara aktif.

Tabel 2 Tabel Pengujian Keaktifan Domain

Status Pengujian	Jumlah	Keterangan
200 Berhasil	35.089	Peladen merespons dengan benar, domain aktif dan dapat diakses.
302 Pindah Sementara	3	Halaman sementara dialihkan ke alamat lain (*redirect* sementara).
307 Pengalihan Sementara	2	Pengalihan sementara, metode HTTP tetap sama.
307 Redirect	1	Pengalihan otomatis ke alamat lain.
400 Permintaan Salah	143	Peladen tidak memahami permintaan karena formatnya salah.
401 Tidak Diizinkan (Butuh Login)	3.195	Diperlukan autentikasi; halaman hanya bisa diakses setelah masuk.
403 Dilarang Akses	3.177	Akses ditolak oleh peladen; biasanya dibatasi oleh *firewall* atau aturan keamanan.
404 Tidak Ditemukan	875	Halaman atau fail tidak ada di peladen.
405 Metode Tidak Diizinkan	2	Jenis permintaan (GET/POST) tidak diizinkan.
409 Terjadi Konflik	2	Terjadi benturan data atau versi.
410 Sudah Dihapus	16	Halaman atau fail telah dihapus secara permanen.
421 Permintaan Salah Arah	3	Permintaan dikirim ke peladen yang salah.

Status Pengujian	Jumlah	Keterangan
466 Sertifikat Tidak Valid	1	Sertifikat keamanan (TLS/SSL) tidak sah.
468 Token / Tanda Tangan Tidak Valid	77	Kesalahan autentikasi; token atau tanda tangan digital tidak valid.
500 Kesalahan Peladen	1.028	Kesalahan umum di sisi peladen.
502 Gerbang Buruk (*Bad Gateway*)	312	Peladen perantara menerima respons yang salah dari peladen tujuan.
503 Layanan Tidak Tersedia	720	Peladen sedang sibuk, dalam perbaikan, atau melebihi kapasitas.
504 Waktu Tunggu Habis (*Gateway Timeout*)	7	Peladen tidak merespons dalam batas waktu tertentu.
508 Terjadi Putaran (*Loop*)	4	Terjadi siklus tak berujung dalam pengalihan atau konfigurasi peladen.
509 Batas Bandwidth Tercapai	1	Kuota lalu lintas peladen habis (*hosting limit*).
520 Kesalahan Tidak Dikenal	73	Kesalahan umum atau tak dikenal (biasanya dari CDN seperti Cloudflare).
521 Peladen Asal Tidak Merespons	125	Peladen utama tidak merespons permintaan dari sistem perantara.
522 Koneksi Habis Waktu	2	Koneksi ke peladen asal terlalu lama dan gagal.
523 Peladen Asal Tidak Dapat Dicapai	210	Peladen asal tidak dapat dijangkau (masalah DNS atau *routing*).
525 Gagal Negosiasi SSL	131	Gagal saat melakukan koneksi aman (SSL/TLS *handshake*).
526 Sertifikat SSL Tidak Sah	306	Sertifikat SSL peladen tidak valid atau kadaluarsa.
530 Situs Diblokir / Dibekukan	23	Situs diblokir atau dibekukan oleh penyedia layanan.
Tidak Ada Keterangan	115.296	Domain gagal diakses sama sekali (peladen mati, DNS bermasalah, atau waktu habis).
Total Domain	**160.824**	**Total domain yang diuji.**

Kategori dengan jumlah terbesar adalah "Tidak Ada Keterangan" sebanyak 115.296 domain, atau sekitar 71,7% dari total. Ini menunjukkan bahwa domain-domain tersebut gagal dihubungi, tidak merespons, atau tidak memiliki peladen aktif. Dalam konteks pemantauan infrastruktur digital, angka ini menunjukkan tingkat inaktivitas yang tinggi dan kemungkinan besar

mencerminkan banyak domain yang telah kedaluwarsa, dinonaktifkan, atau tidak lagi dikelola.

Dari sisi kesalahan akses, terdapat pola yang menarik. Kode 401 (Tidak Diizinkan / Butuh Login) dan 403 (Dilarang Akses) muncul paling banyak di antara kategori *error*, masing-masing dengan 3.195 dan 3.177 domain. Ini menandakan banyak situs masih berfungsi, tetapi hanya bisa diakses dengan kredensial tertentu, seperti halaman *login*, area admin, atau panel internal. Kode 404 (Tidak Ditemukan) muncul pada 875 domain, menunjukkan situs aktif, tetapi tidak memiliki konten yang dapat ditampilkan. Sementara itu, 400 (Permintaan Salah), 405 (Metode Tidak Diizinkan), dan 410 (Sudah Dihapus) muncul dalam jumlah kecil dan tidak berpengaruh signifikan terhadap total keseluruhan.

Beberapa domain juga menunjukkan kesalahan di sisi peladen. Tercatat 1.028 domain mengalami 500 (Kesalahan Peladen), diikuti 720 domain dengan 503 (Layanan Tidak Tersedia), serta 312 domain dengan 502 (Gerbang Buruk). Kesalahan-kesalahan ini umumnya mengindikasikan gangguan di sisi *backend*, seperti kelebihan kapasitas, kesalahan konfigurasi, atau perawatan peladen. Selain itu, ditemukan pula indikasi masalah keamanan pada beberapa domain. Sebanyak 306 domain memiliki sertifikat SSL yang tidak sah (526), dan 131 domain gagal melakukan negosiasi SSL (525). Ini menunjukkan bahwa sebagian situs belum menerapkan konfigurasi HTTPS dengan benar atau menggunakan sertifikat kadaluwarsa.

Ada juga 77 domain dengan kesalahan token atau tanda tangan tidak valid (468), yang berkaitan dengan autentikasi sistem atau API yang tidak sesuai. Sejumlah kecil domain juga terdeteksi dalam status pengalihan seperti 301, 302, dan 307, yang menunjukkan situs-situs tersebut masih aktif tetapi sudah berpindah alamat. Meskipun jumlahnya kecil, kategori ini menandakan adanya aktivitas pemeliharaan atau transisi sistem di sebagian domain.

Secara keseluruhan, hasil ini menunjukkan bahwa mayoritas domain yang diuji berada dalam kondisi tidak aktif atau tidak responsif. Hanya sebagian kecil yang benar-benar berfungsi dan dapat diakses secara publik. Pola yang muncul memperlihatkan dominasi situs-situs dengan pembatasan akses (*login* atau larangan publik), disusul oleh situs yang mengalami kesalahan konfigurasi atau kegagalan server. Tingginya jumlah domain yang tidak lagi aktif juga menandakan rendahnya tingkat keberlanjutan infrastruktur digital dalam himpunan domain yang diuji, di mana lebih dari dua pertiga sudah tidak memiliki layanan web yang berjalan.

Ketidaksesuaian Aturan Penulisan Domain

Menurut Lampiran I Permenkominfo Nomor 5 Tahun 2015 tentang Registrar Nama Domain Instansi Penyelenggara Negara, ditegaskan bahwa:

> *"Format penamaan nama domain instansi penyelenggara negara wajib menggunakan karakter nama lembaga atau unit kerja yang bersangkutan, dan untuk keperluan pembedaan fungsi internal dapat menggunakan subdomain yang mencerminkan fungsi atau unit, seperti 'sekretariat', 'setjen', 'bappeda', 'dprd-kalteng.go.id', atau 'sekretariat.kpu-jatim.go.id'."*

Ketentuan ini secara eksplisit menegaskan bahwa penamaan domain dan subdomain milik instansi pemerintah harus mencerminkan identitas kelembagaan secara sah, bukan sekadar urutan teknis dalam sistem DNS.

Berdasarkan temuan terhadap 160.824 domain dan subdomain yang menggunakan akhiran .go.id, hanya 2.837 di antaranya yang tergolong domain utama, sedangkan sisanya merupakan subdomain dari unit-unit kerja lembaga negara. Secara struktural, data ini menunjukkan bahwa ekosistem domain pemerintah di Indonesia sangat luas dan tersebar di berbagai tingkatan birokrasi. Dari sudut pandang keamanan digital, jumlah subdomain yang besar juga memperluas permukaan serangan *(attack surface)* yang perlu diawasi. Setiap subdomain yang aktif tanpa koordinasi terpusat berpotensi menjadi titik masuk bagi penyusupan atau eksploitasi apabila sistem keamanannya tidak dikelola secara seragam.

Tabel 3 Penulisan Domain

Penulisan Sub Domain	Jumlah
Angka	1.650
Karakter	1
Sesuai	159.173
Total Domain	160.824

Dari hasil temuan tersebut diketahui bahwa 159.173 domain (sekitar 99%) telah mengikuti kaidah penamaan sesuai regulasi, sedangkan 1.651 domain (sekitar 1%) tidak memenuhi ketentuan. Dari jumlah itu, 1.650 subdomain diawali dengan angka dan 1 subdomain menggunakan karakter tidak sah. Contoh pelanggaran dapat ditemukan pada format seperti 1.kpu-pinrangkab.go.id dan 10-situs-poker-online-terpercaya.mandala.biakkab.go.id. Meskipun sebagian masih aktif (75 domain aktif dari 80 yang diperiksa),

bentuk penamaan semacam ini tidak mencerminkan identitas kelembagaan sebagaimana dimaksud dalam Lampiran I Permenkominfo No. 5/2015.

Dari perspektif keamanan digital, penyimpangan format tersebut menunjukkan adanya ketidaktertiban administratif dan kerentanan teknis, sebab pola penamaan yang menyimpang dari konvensi resmi sering muncul dalam konteks injeksi konten, domain *shadowing*, atau *phishing* yang memanfaatkan kemiripan struktur domain pemerintah untuk menipu pengguna. Subdomain yang dibuat tanpa otorisasi atau pengawasan pusat juga dapat menandakan lemahnya pengendalian akses dan dokumentasi DNS di lingkungan instansi pemerintah.

Tabel 4 Status Aktif Subdomain dengan Angka

Subdomain yang Diawali Angka	Jumlah
Aktif	75
Tidak Aktif	5
Total Subdomain	80

Dalam konteks keamanan digital nasional, temuan ini memperlihatkan bahwa pengelolaan domain pemerintah diduga masih bersifat desentralistik dan belum sepenuhnya konsisten. Banyak instansi, terutama di tingkat daerah, mengelola subdomainnya sendiri tanpa mekanisme pengecekan berkala terhadap kesesuaian format dan fungsi. Akibatnya, domain-domain yang tidak sesuai ketentuan tetap aktif dan berpotensi menjadi media serangan, misalnya melalui eksploitasi DNS, penyisipan skrip berbahaya, atau pengalihan lalu lintas *(redirect)* ke situs tidak sah. Kasus subdomain dengan kata kunci komersial atau perjudian yang muncul di bawah domain go.id menunjukkan kemungkinan kompromi sistem atau kesalahan konfigurasi peladen yang dapat menurunkan kredibilitas digital lembaga pemerintah dan kepercayaan publik terhadap situs resmi negara.

Dengan demikian, hasil temuan ini menegaskan bahwa Permenkominfo No. 5 Tahun 2015 perlu dipahami tidak hanya sebagai pedoman administratif, tetapi juga sebagai landasan kebijakan keamanan digital nasional. Tata kelola domain pemerintah memerlukan penguatan koordinasi antar-instansi agar seluruh subdomain yang menggunakan akhiran .go.id benar-benar mencerminkan lembaga dan fungsi resmi pemerintah.

Indikasi Injeksi

Dari total 160.824 domain dan subdomain pemerintah yang teridentifikasi, sebanyak 9.141 subdomain dipilih untuk dianalisis secara mendalam. Analisis ini bertujuan untuk memetakan tingkat keamanan dan potensi penyisipan konten berbahaya.

Tabel 5 Daftar Subdomain Terinjeksi

Subdomain Terinjeksi	Jumlah Subdomain
Ditemukan	3.625
Tidak dapat Diakses	4.935
Tidak Ditemukan	581
Jumlah Subdomain	9.141

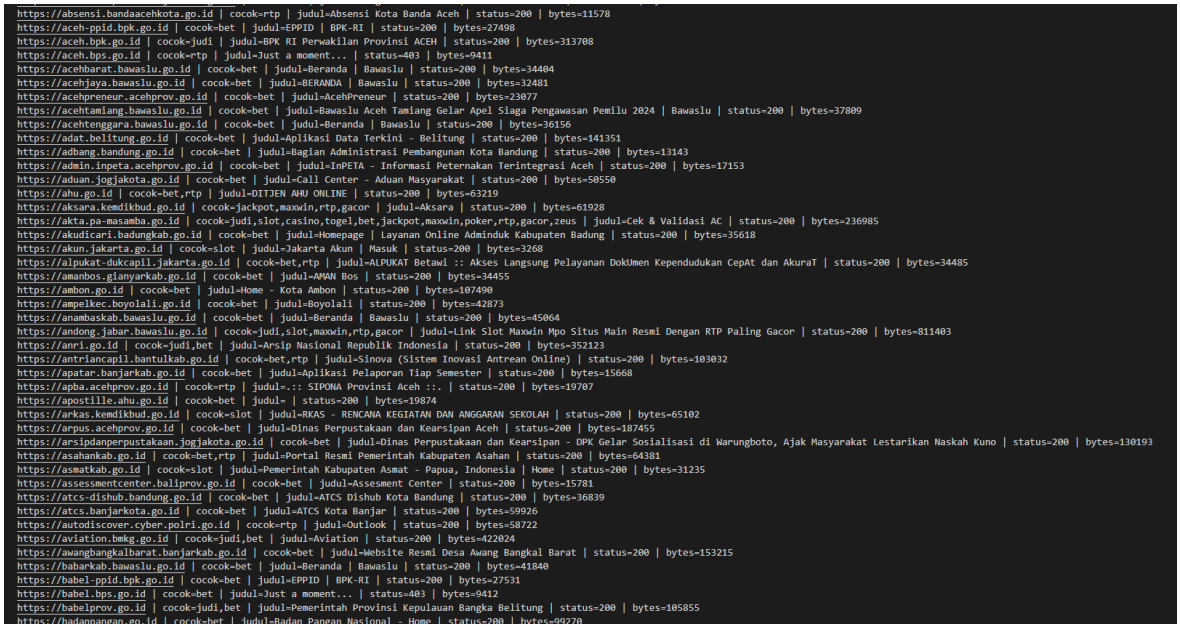
Hasil pemeriksaan menunjukkan bahwa 3.625 subdomain (39,66%) terindikasi mengalami injeksi tautan, sementara 4.935 subdomain (53,99%) tidak dapat diakses pada saat proses analisis dilakukan, dan 581 subdomain (6,36%) dinyatakan bersih tanpa temuan injeksi. Dari total subdomain yang terinjeksi, hanya 20 subdomain (0,55%) yang digunakan untuk analisis lanjutan karena menunjukkan tingkat serangan paling tinggi, sedangkan 3.605 subdomain (99,45%) lainnya belum dianalisis secara detail.

Tabel 6 Subdomain yang Teridentifikasi Menautkan Situs Web Judol

Subdomain Diselidiki	Jumlah Tautan Judol
https://akta.pa-masamba.go.id	2.233
https://banjarkota.bawaslu.go.id	228
https://bappeda.baritoselatankab.go.id	145
https://batanghari.bawaslu.go.id	74
https://bengkulutengahkab.bawaslu.go.id	192
https://dilmilti3-surabaya.go.id	231
https://dindikbud.demakkab.go.id	1.887
https://dinperkim.demakkab.go.id	1.469
https://disdikbud.bengkuluselatankab.go.id	102
https://jakarta.bawaslu.go.id	19
https://jakarta.go.id	2
https://jdih.pn-masamba.go.id	10
https://kejari-sidoarjo.go.id	361
https://kerinci.bawaslu.go.id	156
https://pa-masamba.go.id	26

https://ppid.jateng.bawaslu.go.id	57
https://rskgm.bandung.go.id/	6
https://rsmajenang.cilacapkab.go.id	18
https://samosir.bawaslu.go.id	141
https://www.pa-bangko.go.id	934
Jumlah Keseluruhan	8.291

Dari hasil penelusuran terhadap 20 subdomain pemerintah berakhiran .go.id, ditemukan total 7.513 tautan bertema judol yang tertanam di halaman-halaman situs resmi lembaga negara maupun pemerintah daerah. Seluruh subdomain yang diperiksa menunjukkan indikasi injeksi aktif, meskipun tingkat penyebarannya bervariasi dari ribuan hingga hanya puluhan tautan. Temuan ini memperlihatkan bahwa serangan siber berbentuk penyisipan tautan judol telah menjangkau berbagai sektor pemerintahan, mulai dari lembaga peradilan, dinas pendidikan, hingga pengawasan pemilu di tingkat daerah.



Gambar 2: Temuan tautan judi online pada situsweb pemerintah (sumber: SAFEnet)

Kasus paling berat terjadi pada akta.pa-masamba.go.id dengan 2.232 tautan judol, diikuti dindikbud.demakkab.go.id (1.427 tautan), dan dinperkim.demakkab.go.id (1.415) tautan. Ketiganya menyumbang hampir dua pertiga dari total seluruh tautan judol yang ditemukan, menunjukkan adanya serangan serius terhadap sistem situs web. Sementara itu, pa-bangko.go.id juga menunjukkan jumlah tinggi dengan 934 tautan, menjadikannya salah satu situs paling terdampak setelah Masamba dan Demak.

Beberapa situs lain mengalami serangan tingkat sedang, dengan jumlah tautan judol di kisaran ratusan. Misalnya, kejari-sidoarjo.go.id dengan 361 tautan, banjarkota.bawaslu.go.id dengan 228 tautan, bengkulutengahkab.bawaslu.go.id dengan 191 tautan, dan kerinci.bawaslu.go.id dengan 156 tautan. Situs-situs ini masih menampilkan halaman resmi dan tampak berfungsi normal, tetapi di dalam struktur HTML-nya tersembunyi tautan-tautan judol yang sulit terdeteksi secara kasat mata. Jenis injeksi ini seringkali merupakan hasil dari skrip otomatis yang menyusup melalui *plugin*, direktori *file upload*, atau tema situs yang tidak diperbarui.

Selain itu, terdapat pula situs yang baru mengalami injeksi dalam skala kecil, dengan jumlah tautan di bawah 50. Contohnya pa-masamba.go.id dan dilmilti3-surabaya.go.id masing-masing 22 tautan, rsmajenang.cilacapkab.go.id (18 tautan), jdih.pn-masamba.go.id (10 tautan), dan rskgm.bandung.go.id (4 tautan). Walaupun jumlahnya sedikit, kategori ini tidak boleh diabaikan karena menunjukkan indikasi awal penyusupan, di mana pelaku biasanya sedang menguji celah sistem sebelum memperluas serangan.

Dari sisi lembaga, Badan Pengawas Pemilu (Bawaslu) menjadi instansi dengan jumlah subdomain terdampak terbanyak. Terdapat tujuh situs berbeda yang mengalami serangan, yaitu banjarkota.bawaslu.go.id, batanghari.bawaslu.go.id, kerinci.bawaslu.go.id, bengkulutengahkab.bawaslu.go.id, ppid.jateng.bawaslu.go.id, jakarta.bawaslu.go.id, dan samosir.bawaslu.go.id. Hal ini menunjukkan adanya pola serangan berulang terhadap struktur sistem yang seragam di berbagai wilayah, kemungkinan karena penggunaan *hosting*, *content management system* (CMS), atau konfigurasi keamanan yang sama. Sementara itu, dua situs di Kabupaten Demak (Dindikbud dan Dinperkim) kembali menjadi yang paling parah terinjeksi, menandakan adanya serangan sistematis pada satu lingkungan peladen yang sama.

Secara keseluruhan, hasil ini memperlihatkan bahwa injeksi tautan judol pada situs pemerintah telah menyebar luas dengan tingkat keparahan berlapis. Ada situs yang telah sepenuhnya dikuasai dengan ribuan tautan, ada yang terinjeksi sebagian dengan ratusan tautan, dan ada pula yang baru menunjukkan gejala awal. Fenomena ini menunjukkan bahwa keamanan digital situs pemerintah masih sangat rentan, terutama pada sistem berbasis CMS yang tidak diperbarui dan server dengan kontrol keamanan rendah.

Kata Kunci yang Digunakan

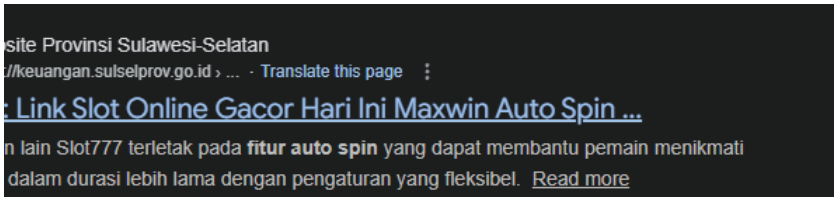
Temuan terkini menunjukkan bahwa pola penyebaran konten judi daring di subdomain instansi pemerintahan berlangsung melalui dua jalur utama,

yakni kata kunci *(keyword seeding)* dan judul berita palsu *(narrative injection)*. Kedua metode ini saling melengkapi: kata kunci berfungsi untuk menembus sistem indeks mesin pencari secara teknis, sementara judul berita digunakan untuk menarik perhatian pengguna manusia melalui narasi lokal yang tampak realistis.

Berdasarkan analisis linguistik dari ratusan entri temuan, dapat disimpulkan bahwa penyebaran ini mengikuti pola yang sangat terstruktur dan dapat dikelompokkan dalam beberapa klaster leksikal utama.

Klaster pertama adalah Teknis Promo dengan istilah seperti RTP JAYA805, RTP MACANASIA, rtplive, rtpirit4d, rtpindobit, dan rtphoki. Istilah RTP (return to player) digunakan untuk menciptakan kesan ilmiah dan profesional dalam narasi seperti "RTP 96%" atau "tingkat kemenangan 97%". Pola ini disebut *technical lure*, yakni penggunaan istilah teknis untuk memberikan legitimasi palsu. Dalam banyak kasus, RTP dipasangkan dengan nama merek lokal seperti JAYA805 dan MACANASIA untuk menipu pengguna agar mengira situs tersebut sah atau berlisensi.

Selanjutnya, klaster TOTO/TOGEL/LOTTO (Angka 4D) meliputi temuan seperti toto 4d, bandungtoto, malukutoto, manadototo, Winsortoto, Cendanatoto, CINDOTOTO, dan CHINDOTOTO. Istilah-istilah ini menunjukkan aktivitas taruhan angka yang menggunakan ejaan bervariasi dan nama wilayah untuk menghindari filter otomatis. Strategi ini merupakan bentuk *linguistic obfuscation* yang sekaligus memperkuat segmentasi pasar lokal Indonesia. Karena banyak menggunakan nama daerah, klaster ini dapat dimanfaatkan untuk *geo-tagging*, yaitu pemetaan asal operasi jaringan berdasarkan konteks linguistik domain yang disusupi.



Pada klaster SLOT (Permainan Utama), istilah seperti slot gacor hari ini, slot online, slot88, slot777, Slot Dana, Slot Qris, dan SLOT PULSA mendominasi dataset. Kata "slot" menjadi penanda inti *(core lexical indicator)* dari seluruh ekosistem promosi. Variasi seperti Slot Dana atau Slot Pulsa menunjukkan kemampuan jaringan untuk menyesuaikan diri dengan sistem pembayaran populer di Indonesia. Adapun frasa seperti slot gacor hari ini menunjukkan pola *real-time lure* yang memanfaatkan kesan waktu agar terlihat dinamis. Kombinasi "slot" dengan nominal kecil seperti 10K dirancang untuk menurunkan hambatan psikologis calon korban dan memicu klik impulsif.

Klaster BET/WIN/VIP (Taruhan dan Insentif) juga banyak ditemukan, misalnya pada ATLASBET88, CUANWIN138, BOSS88, Maharaja188, serta istilah "jackpot" dan "spin gratis" yang muncul di narasi berita. Klaster ini menggambarkan *clickbait incentive* yang menjanjikan kemenangan cepat dan hadiah besar. Kata "cuan", slang populer Indonesia untuk keuntungan, memperlihatkan penyesuaian budaya yang memperkuat daya tarik emosional. Contoh narasi seperti "**Penjual gorengan temukan pola viral Gates of Olympus, dari Rp80.000 jadi Rp212.000.000**" menunjukkan perpaduan kata kunci kemenangan dengan cerita lokal untuk menipu pengguna melalui social engineering berbasis empati.

Klaster 4D (Penanda Togel Indonesia) seperti Senior4d dan Kapital4D menandakan jaringan lokal yang menggunakan pola angka empat digit khas Asia Tenggara. Ini menjadi jejak geografis yang berguna untuk pelacakan jaringan. Sementara itu, klaster Angka Khas *(Numerik Branding)* meliputi nama-nama seperti asia99, ora78, panen77, slot777, CUANWIN138, ATLASBET88, JAYA805, dan MACANASIA. Angka-angka seperti 77, 88, 99, 138, dan 303 merupakan simbol keberuntungan Asia yang digunakan sebagai bagian dari identitas merek. Pola huruf-angka ini sering diproduksi secara massal menggunakan *domain generation algorithm* (DGA) manual untuk menghindari pemblokiran otomatis.

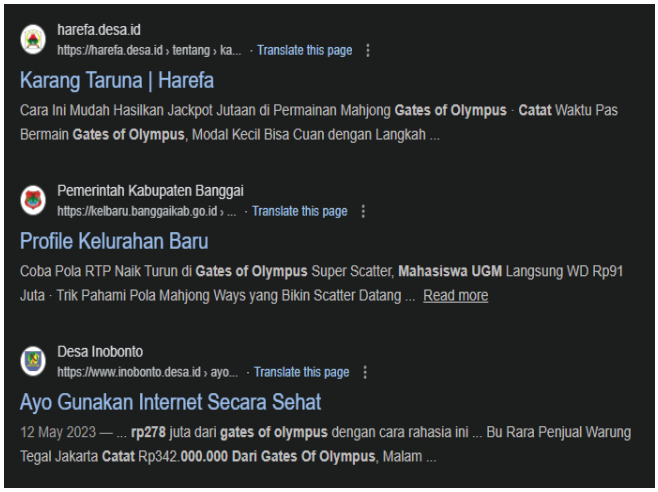
Selain itu, muncul pula klaster Slang/Promosi (Bahasa Emosional) seperti gacor, maxwin, cuan, dan hadiah. Istilah ini merupakan *social engineering lexical indicators* yang dirancang untuk memancing emosi keserakahan dan euforia kemenangan. Contohnya, frasa "slot gacor" memberi kesan bahwa ada momen keberuntungan yang bisa diprediksi, sedangkan "maxwin" digunakan sebagai simbol status di komunitas daring. Kata-kata ini kerap muncul bersama narasi "Viral!", "Tak Masuk Akal!", atau "Auto Sultan!", yang menandakan upaya eksploitasi psikologis pengguna.

Pada klaster HOKI/JP (Keberuntungan Lokal), istilah seperti Hokiwin33 dan hokislot menunjukkan sinkretisme budaya Indonesia-Tionghoa. Penggunaan kata "hoki" (keberuntungan) dan singkatan "JP" (jackpot) menandakan segmentasi pasar lokal dengan pendekatan kultural. Selanjutnya, klaster QQ/BOLA/SPORT (Olahraga dan Poker) dengan contoh SV388 dan UFABET memperlihatkan ekspansi jaringan ke sektor taruhan olahraga dan sabung ayam, mengindikasikan keterhubungan lintas negara antara operator judi Asia.

Klaster lain yang menonjol adalah Brand/Ikon Mitologi (Visual Imitation) dengan contoh seperti Zeus, Gates of Olympus, Starlight Princess, Sweet Bonanza, dan Wild Bandito. Nama-nama ini merupakan hasil *brand*

spoofing terhadap game internasional seperti PGSoft atau Pragmatic Play. Penggunaan ikon mitologi seperti Zeus atau Medusa dimaksudkan untuk meniru citra profesional dan mengaburkan perbedaan antara situs resmi dan palsu.

Sementara itu, klaster Merek Lokal/Nasional seperti KapitalSlot, Maharaja188, duniacash, Cindo Toto, manadototo, malukutoto, dan bandungtoto menunjukkan rantai distribusi konten ilegal yang beroperasi dengan gaya penamaan Indonesia. Penyebaran ini bersifat domestik dan sering kali menumpang pada domain atau subdomain instansi pemerintah, menandakan lemahnya sistem keamanan situs publik di tingkat *server* dan CMS.



Selain penyebaran berbasis kata kunci, temuan juga menunjukkan adanya pola judul berita palsu yang digunakan untuk mengelabui pengguna. Narasi seperti **"Surabaya, Pedagang Nasi Bebek Raih Rp187.350.000 dari Mahjong Ways 2"**, **"Viral! Mahasiswi UGM Catat Rp278.000.000 dari Gates of Olympus"**, atau **"Tukang Bakso Blitar Bawa Pulang Rp121.700.000 dari Provider PGSoft Joyslot88"** menggabungkan nama kota, profesi umum, jumlah uang, dan nama platform judi. Pola ini menciptakan *social proof* palsu, seolah-olah keberuntungan itu nyata dan dialami oleh warga biasa. Secara linguistik, judul-judul ini mengandung kombinasi *trigger word* (Viral, Tak Masuk Akal, Trik, dll) dan entitas finansial (Rp...) yang efektif meningkatkan klik serta penyebaran organik melalui pencarian.

Keseluruhan analisis menunjukkan bahwa jaringan injeksi ini tidak bersifat acak, melainkan terorganisasi dengan baik melalui struktur linguistik dan visual. Kata kunci digunakan sebagai komponen teknis untuk optimasi mesin pencari, sedangkan judul berita panjang berfungsi sebagai komponen sosial yang membangun kepercayaan semu. Penggabungan istilah teknis (RTP, Scatter, Pola), budaya lokal (Hoki, Cuan, Gacor), dan simbol internasional (Zeus, Olympus, Starlight Princess) membentuk ekosistem yang kompleks.

Dengan memahami setiap klaster dan korelasinya, upaya deteksi dapat diarahkan pada tiga lapisan: leksikal (kata kunci dan pola angka), jenama (kombinasi huruf-angka dan nama permainan), serta naratif (judul panjang dengan pola kota–uang–brand). Pendekatan ini memungkinkan pemetaan

lebih presisi terhadap pola penyebaran, aktor lokal, dan sumber konten berisiko yang menyusup ke dalam ekosistem domain nasional.

Metode Penyebaran

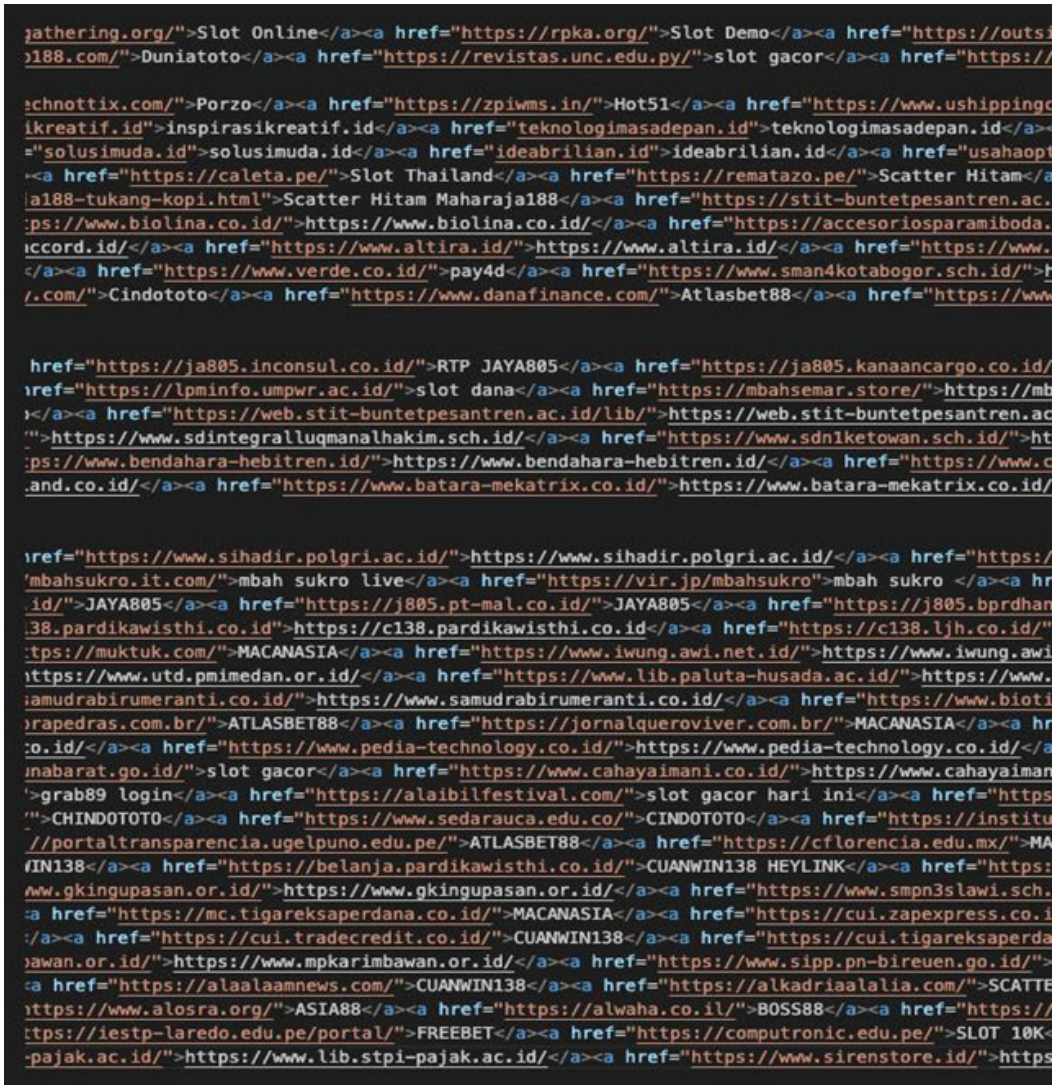
Terdapat dua metode utama dalam penyebaran konten judi daring yang disisipkan ke berbagai domain, termasuk situs lembaga dan perusahaan Indonesia. Metode pertama adalah injeksi langsung berbasis kata kunci sedangkan metode kedua adalah injeksi kalimat naratif melalui artikel palsu. Kedua teknik ini saling melengkapi. Teknik pertama berfungsi memperkuat visibilitas mesin pencari melalui optimasi teknis, sementara teknik kedua menipu pengguna dengan membangun narasi seperti berita lokal.

Tabel 7 Kata Kunci dan Penggunaan Kalimat Penyebaran Judol

Aspek	Penggunaan Kata Kunci	Penggunaan Kalimat
Bentuk Konten	Kata atau frasa pendek seperti MACANASIA, CUANWIN138, Slot Dana, JAYA805	Judul panjang bergaya berita, misalnya "Pedagang Buah Raih Rp215.700.000 dari Mahjong Ways Joyslot88"
Tujuan Utama	Optimasi SEO dan penguatan merek judi di mesin pencari	Penipuan sosial dengan membangun narasi kemenangan palsu
Lokasi Injeksi	Halaman utama atau root domain (.com, .co.id)	Folder internal CMS (misalnya /wp-content/themes/ atau / News/)
Contoh Domain Terdampak	topatrikomas.com, trigunasakti.co.id, tuxtla.com.mx, wintracoperkasa.com	umtas.ac.id (puluhan artikel di direktori themes dan News)
Karakteristik Teknis	Sederhana, statis, dan tersembunyi di metadata atau tag HTML	Kompleks, dinamis, berupa file HTML baru dengan struktur naratif
Target Utama	Mesin pencari (Google, Bing)	Pengguna manusia dan algoritma pencarian sekaligus
Efek yang Dihasilkan	Meningkatkan visibilitas merek judi secara otomatis	Meningkatkan klik, kepercayaan palsu, dan penyebaran konten cepat

Pada metode injeksi kata kunci, pola yang ditemukan bersifat pendek dan langsung, biasanya hanya berupa satu kata atau frasa yang mengandung istilah perjudian seperti Slot Dana, MACANASIA, CUANWIN138, ATLASBET88,

atau JAYA805. Injeksi semacam ini sering muncul di domain aktif milik perusahaan sah seperti topatrikomas.com, trigunasakti.co.id, tuxtla.com.mx, atau wintracoperkasa.com. Teknik ini bekerja dengan menanamkan kata kunci ke dalam halaman utama atau metadata situs agar muncul di hasil pencarian Google saat pengguna mencari istilah terkait judi. Dengan cara ini, situs yang tampak normal atau profesional menjadi jembatan tersembunyi untuk memperkuat posisi *brand* judi di mesin pencari. Karakteristiknya statis dan sederhana. Tidak ada narasi panjang, hanya kata kunci tunggal sebagai umpan SEO.



Gambar 3: Tangkapan Layar Injeksi pada laman Website (Sumber: SAFEnet)

Sebaliknya, metode injeksi narasi menampilkan pendekatan yang jauh lebih kompleks. Pola ini ditemukan secara masif pada domain umtas.ac.id, di mana puluhan halaman palsu disimpan di dalam direktori wp-content/themes/ dan News/. Setiap halaman berisi narasi panjang bergaya berita

dengan judul seperti "**Pedagang Buah Raih Rp215.700.000 dari Mahjong Ways Joyslot88**", "**Viral! Mahasiswi UGM Catat Rp278.000.000 dari Gates of Olympus**", atau "**Tangerang: Sopir Pribadi Menang Rp399.000.000 Berkat Pola RTP 97% di Mahjong Ways 2**".

Artikel-artikel ini disusun menyerupai laporan media, lengkap dengan nama kota, profesi sehari-hari, dan jumlah uang spesifik dalam rupiah. Hasilnya adalah kesan bahwa laporan tersebut memang benar. Tujuannya bukan hanya menaikkan peringkat pencarian, tetapi juga membangun kepercayaan emosional melalui *social proof* palsu, membuat pembaca merasa kemenangan besar itu nyata dan mungkin mereka alami sendiri.

Secara teknis, perbedaan keduanya terlihat dari lokasi dan mekanisme injeksi. *Keyword injection* terjadi di halaman utama atau *direktori root* domain yang relatif stabil, sedangkan *narrative injection* dilakukan dengan menambah file HTML di struktur internal Wordpress, terutama pada direktori tema yang rentan karena kelemahan plugin atau izin akses file. Perbedaan ini juga mencerminkan targetnya. Injeksi berbasis kata kunci menipu mesin pencari untuk meningkatkan ranking, sementara injeksi naratif menipu manusia dengan memanfaatkan psikologi keingintahuan, euforia, dan iming-iming keuntungan cepat.

Kedua metode ini menunjukkan bahwa jaringan penyebar konten judi daring bekerja dalam sistem yang saling terhubung. *Keyword injection* berperan membangun fondasi indeks SEO melalui ribuan situs yang tampak sah, sedangkan *narrative injection* digunakan untuk menyalurkan pesan utama dengan cara lebih persuasif. Kombinasi antara keduanya membuat kampanye injeksi sulit dideteksi secara otomatis. Karena sebagian besar domain tetap terlihat normal di permukaan, tetapi menyimpan tautan dan artikel tersembunyi yang mendistribusikan konten ilegal secara sistematis.

Pemindaian Sucuri

Untuk memperkuat temuan terhadap situs-situs web pemerintah yang menjadi korban injeksi kata kunci maupun narasi, kami juga melakukan pemindaian secara daring. Tujuan kegiatan ini adalah untuk menemukan sejauh mana tingkat kerentanan situs-situs tersebut. Salah satu platform yang kami gunakan adalah sucuri.[3] Platform ini juga memeriksa apakah sebuah situs memiliki masalah keamanan, termasuk *malware*, virus, perangkat lunak kedaluwarsa, dan kode berbahaya.

Hasil pemindaian diperlihatkan dalam lima tingkat kerentanan, yaitu

3 *https://sitecheck.sucuri.net/*

Sangat Rendah, Rendah, Sedang, Tinggi, dan Kritis. Situs web yang memiliki tingkat kerentanan Sangat Rendah berarti paling aman, sedangkan Kritis berarti paling rentan. Hasil pemindaian terhadap situs-situs web tersebut diperlihatkan di Tabel 8.

Tabel 8 Hasil Pemindaian Sucuri

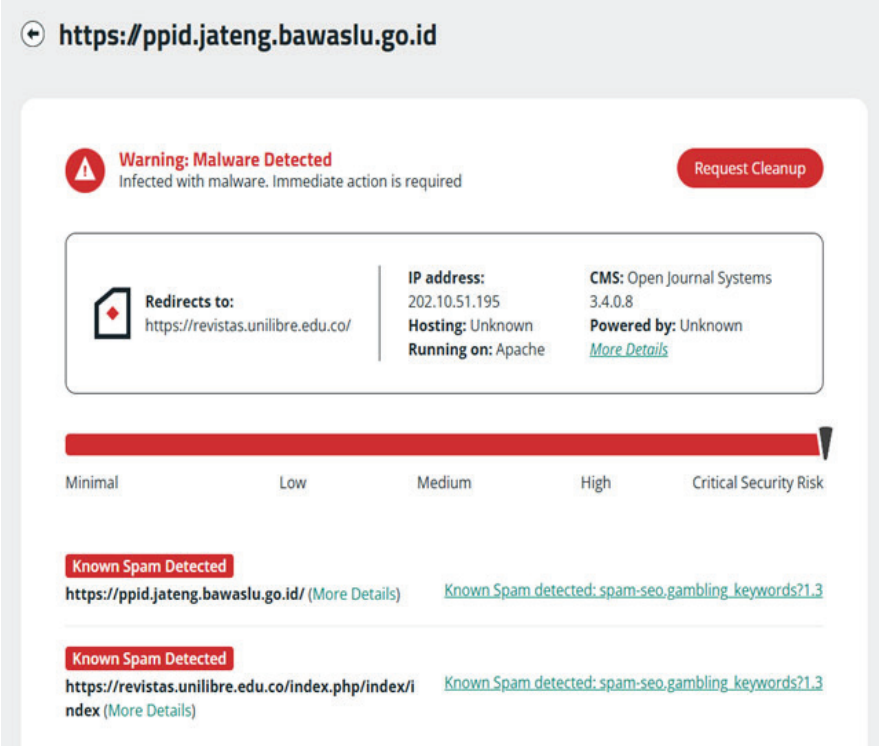
Subdomain Diselidiki	Status Penilaian Sucuri
https://akta.pa-masamba.go.id	Critical Security Risk
https://banjarkota.bawaslu.go.id	Medium
https://bappeda.baritoselatankab.go.id	Medium
https://batanghari.bawaslu.go.id	Medium
https://bengkulutengahkab.bawaslu.go.id	Medium
https://dilmilti3-surabaya.go.id	Medium
https://dindikbud.demakkab.go.id	Medium
https://dinperkim.demakkab.go.id	Medium
https://disdikbud.bengkuluselatankab.go.id	Medium
https://jakarta.bawaslu.go.id	Medium
https://jakarta.go.id	Medium
https://jdih.pn-masamba.go.id	Medium
https://kejari-sidoarjo.go.id	Low
https://kerinci.bawaslu.go.id	Medium
https://pa-masamba.go.id	Medium
https://ppid.jateng.bawaslu.go.id	Critical Security Risk
https://rskgm.bandung.go.id/	Medium
https://rsmajenang.cilacapkab.go.id	Medium
https://samosir.bawaslu.go.id	Medium
https://www.pa-bangko.go.id	Medium

Pengecekan Pemblokiran

Berdasarkan temuan dari kumpulan situs judol yang tertaut pada domain .go.id, penelurusan lebih lanjut dilakukan guna memverifikasi aksesibilitas situs terkait. Penelurusan dilakukan dengan mengakses semua situs yang terindikasi terdapat muatan judol, kemudian melakukan pengecekan apakah terdapat pembatasan konten atau akses internet, atau masih bisa diakses secara bebas.

Proses verifikasi dari 5.159 situs menunjukkan hanya terdapat 11% situs yang terblokir. Sementara itu, hampir 50% situs judol masih dapat diakses secara

luas dan bebas dengan penyedia layanan internet di Indonesia. Sisanya, terdapat gangguan akses dalam sitem situs web atau peladen situs terkait. Ragamnya bermacam-macam. Ada situs yang sudah tidak aktif, pelarangan akses dari situs terkait, dan mengeluarkan informasi kesalahan lainnya.



Gambar 2: Tangkapan Layar hasil pengecekan Sucuri pada salah satu Situsweb (Sumber: SAFEnet)

Hal ini menunjukkan bahwa pemblokiran situs judol belum berjalan secara efektif. Tampak dari situs judol yang tersebar dan tertanam pada situs pemerintahan dengan domain .go.id, masih bisa diakses secara mudah, bebas dari pemblokiran.

Tabel 9 Status Situs Temuan

Status Domain	Kode http	Jumlah link tertaut
Berhasil Akses (Tidak Diblokir)	200	2500
Diblokir ISP	HJK	605
Diblokir/Dibekukan	530	1
Dilarang Akses	403	576
Invalid SSL Cert	526	2
Kesalahan Server	500	41

Status Domain	Kode http	Jumlah link tertaut
Kesalahan Tidak Dikenal	520	534
Layanan Tidak Tersedia	503	28
Origin Down	521	1
Pengalihan Sementara	307	2
Pindah Permanen	301	536
Pindah Sementara	302	253
SSL Handshake Failed	525	4
Sudah Dihapus	410	1
Terjadi Konflik	409	1
Tidak Diizinkan	401	1
Status Lainnya	303 | 308 | 402 | 406 | 509	26
Tidak Ditemukan	404	47
Total Domain		**5159**

Mekanisme Penanganan

Untuk mengonfirmasi temuan awal yaitu situs-situs web pemerintah yang disisipi iklan dan tautan, kami melaksanakan diskusi daring pada 7 November 2025. Diskusi ini menghadirkan perwakilan Komdigi, Pusilkom UI, dan komunitas keamanan digital Ngesec. Kami juga mengundang Badan Siber dan Sandi Negara (BSSN), Siber Polri, dan Bawaslu, tetapi mereka tidak hadir.

Salah satu topik mengemuka dalam diskusi ini adalah sejauh mana pemerintah menangani serangan-serangan terhadap situs web pemerintah. Komdigi, melalui peran pengawasan dan pengendalian konten, memiliki mekanisme spesifik dalam menangani injeksi judol pada situs web pemerintah. Pendekatan ini berbeda dengan penanganan situs judol murni.

Pertama dari sisi pemantauan. Komdigi memiliki tim Patroli Siber yang bertugas untuk menginventarisasi situs-situs ilegal. Ketika konten sisipan judol ditemukan, tim ini akan melapor kepada Direktorat Jenderal Teknologi Pemerintahan Digital (Ditjen TPD) untuk dikoordinasikan dengan pemilik website agar segera melakukan penghapusan atau menonaktifkan situs sementara.

Kedua melalui pemblokiran secara selektif. Komdigi tidak mungkin memblokir seluruh domain pemerintahan ke dalam basis data *blacklist* Trust Positif. Penanganan dilakukan dengan berkoordinasi terlebih dahulu dengan pengelola *(webmaster)* situs web atau Dinas Komunikasi dan

Informatika (Diskominfo), lembaga yang bertanggung jawab mengelola situs tersebut, untuk melakukan perbaikan. Pemblokiran hanya dilakukan jika pengelola tidak dapat dikoordinasikan, tidak memiliki akses teknis untuk perbaikan, dan dilakukan dengan seizin pihak pengelola situs web. Tujuannya hanya untuk menutup akses, bukan mematikan domain.

Untuk domain yang memang dimiliki entitas judol dan menggunakan TLD .id (bukan .go.id, .ac.id, dll.), Komdigi bekerja sama dengan PANDI untuk langsung melakukan penutupan total. Artinya, layanan tersebut benar-benar dimatikan dan tidak bisa diakses bahkan dari luar negeri. Tindakan ini pernah dilakukan Komdigi ketika menemukan situs judol menggunakan TLD .id dan tidak diketahui pemiliknya.

Mekanisme pemblokiran di Komdigi mengikuti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik (PP PSTE) dan Permenkominfo Nomor 5 Tahun 2020 tentang PSE Lingkup Privat, khususnya Pasal 13 dan Pasal 15. Prosedurnya adalah setelah situs ilegal ditemukan, tautan dipetakan, dan disampaikan ke bagian infrastruktur untuk dilakukan pemblokiran situs dan/atau alamat protokol (IP).

Tantangannya, situs judol dapat mengganti domain dengan cepat, dan *source code* mereka memungkinkan pengalihan ke domain baru segera setelah diblokir. Selain itu, tidak semua penyedia jasa internet (ISP) di Indonesia mematuhi atau tersinkronisasi secara tepat waktu *(real-time)* dengan pangkalan data Komdigi, yaitu Trust Positif, sehingga memungkinkan situs yang sudah diblokir tetap bisa diakses.

Masalah Utama dan Akar Penyebab

Diskusi daring juga memetakan masalah utama maraknya serangan injeksi judol pada situs web pemerintah yang berakar pada tiga aspek, yaitu tata kelola, sumber daya manusia, dan teknologi.

Tata Kelola

Aspek ini merupakan masalah utama penyebab terjadinya serangan secara masif terhadap situs-situs milik pemerintah. Belum ada *standard operating procedure* (SOP) terpusat yang mewajibkan peninjauan (*review*) situs web pemerintah secara berkala. Hal ini karena tidak semua lembaga pemerintah, terutama di daerah, memiliki *chief information officer* (CIO) yang secara spesifik bertanggung jawab atas keamanan informasi situs secara umum.

Tanpa adanya SOP, maka tidak ada pula pembagian peran antara pemerintah daerah sebagai pembuat dan pemelihara situs web, termasuk keamanannya,

dengan instansi pusat. Pembuatan, pemeliharaan, dan keamanan situs web dengan domain .go.id sepenuhnya menjadi tanggung jawab instansi pusat atau pemerintah daerah yang membuat, bukan Komdigi. Situasi ini diperparah pula dengan tumpang tindih atau saling lempar tanggung jawab yang sering terjadi antara Komdigi dan BSSN, terutama pada saat terjadi serangan siber terhadap aset digital pemerintah.

Teknologi

Salah satu celah kerentanan yang sering dieksploitasi pelaku serangan digital adalah CMS dan peranti situs web lainnya. Banyak lembaga pemerintah menggunakan CMS sejuta umat, Wordpress, karena kemudahan penggunaannya, terutama bagi orang-orang nonteknis. Padahal, sebagai CMS paling populer, Wordpress juga mudah disisipi dengan *javascript* jika celah keamanan sistemnya terdeteksi dan bisa dieksploitasi.

Faktor lain dari aspek teknologi yang membuat situs web rentan adalah sebagian peladen masih menjalankan PHP 5.x–7.0 yang sudah tidak mendapat pembaruan keamanan. Situasi ini meningkatkan risiko eksploitasi dan injeksi kode berbahaya. Ada pula situs-situs web yang menggunakan sertifikat SSL kedaluwarsa atau salah konfigurasi sehingga gagal melakukan SSL *handshake* dan memunculkan peringatan keamanan di peramban.

Kondisi ini diperparah dengan tidak adanya pemeliharaan berkala terhadap situs-situs web tersebut sehingga ketika sejumlah peranti (*tools dan plugin*) sudah kedaluwarsa pun tidak diketahui. Akibatnya, serangan semakin mudah dilakukan.

Sumber Daya Manusia

Jamak jadi tantangan, kapasitas sumber daya manusia di bidang keamanan siber Indonesia relatif masih terbatas, baik dari sisi kualitas maupun kuantitas. Tidak semua pengelola situs web memiliki pengetahuan dan keterampilan teknis sehingga masih belum menerapkan strategi keamanan siber bahkan yang mendasar sekali pun. Praktik keamanan seperti kata sandi yang kuat dan penerapan autentikasi dua langkah masih menjadi prinsip dasar yang dilupakan.

Dari sisi kuantitas, jumlah sumber daya manusia yang memahami dan menerapkan keamanan siber, terutama di lembaga-lembaga pemerintah, juga masih terbatas. Jika toh ada, mereka juga disibukkan dengan tugas-tugas teknis lain yang sering kali tak berhubungan dengan sistem keamanan. Hal ini membuat pengelolaan situs web milik pemerintah pun terabaikan.

Penutup

Kesimpulan

Di tengah gencarnya upaya pemerintah Indonesia memerangi judol, situs-situs web pemerintah justru menjadi korban serangan siber dalam bentuk penyisipan iklan atau tautan situs web judo. Dari sampel 9.141 subdomain yang dianalisis menggunakan sejumlah metode secara detail, hampir 40% atau sekitar 3.625 situs pemerintah positif terinfeksi injeksi tautan judol.

Hanya sekitar 6% situs yang dinyatakan benar-benar bersih. Sisanya? Sebagian besar dalam kondisi mati atau tidak terurus. Yang lebih mengkhawatirkan, dari 20 sampel subdomain dengan tingkat serangan tertinggi, ditemukan setidaknya 7.513 tautan aktif yang mengarahkan pengguna ke situs judol. Injeksi ini merambah ke berbagai sektor sensitif, mulai dari lembaga peradilan, dinas pendidikan, hingga pengawas pemilu di daerah. Situs-situs ini bukan lagi sekadar menyajikan informasi publik, melainkan menjadi "papan iklan gratis" bagi bandar judi.

Untuk menyerang situs-situs web tersebut, pelaku menggunakan strategi sistematis melalui permainan kata-kata (linguistik) dan teknis yang sangat terstruktur melalui dua jalur utama. Pertama, penyebaran kata kunci. Pelaku menanamkan istilah teknis seperti RTP, Scatter, Slot, Togel, hingga nama ikon mitologi seperti Zeus atau Starlight Princess. Tujuannya untuk menggaet korban melalui mesin pencari, seperti Google. Dengan menanam kata kunci ini di situs pemerintah yang punya reputasi tinggi di mata Google, situs judi mereka akan otomatis muncul di halaman utama pencarian.

Kedua, melalui narasi berita palsu. Tak lagi sekadar kata-kata teknis, pelaku juga membuat artikel palsu dengan judul persuasif, provokatif, bombastis, atau narasi lokal yang tampak nyata. Ini adalah teknik tipuan sosial agar pengguna merasa yakin bahwa situs tersebut legal karena berada di bawah payung domain pemerintah.

Kombinasi ini menciptakan ekosistem "simbiosis parasitisme" di mana situs judi meminjam otoritas negara untuk membangun legitimasi palsu di mata korban.

Rapuhnya situs web pemerintah terhadap serangan judol tersebut berakar pada tiga sebab utama, yaitu tata kelola, teknologi, dan sumber daya manusia. Pengelolaan domain pemerintah, terutama di tingkat daerah, cenderung berantakan. Banyak instansi pemerintah mengelola subdomain

sendiri tanpa standardisasi dan mekanisme pemantauan berkala. Akibatnya, banyak "pintu belakang" yang terbuka tanpa pengawasan pusat.

Dari sisi teknologi, terdapat sejumlah kerentanan, termasuk penggunaan CMS yang tidak diperbarui, sistem peladen yang usang, dan konfigurasi sertifikat SSL yang salah. Kerentanan ini menjadi pintu masuk bagi penyerang untuk menyisipkan tautan-tautan terkait judol.

Kurangnya kapasitas sumber daya manusia, baik kualitas maupun kuantitas, membuat benteng pemerintah untuk melawan judol pun semakin rapuh. Pengelola situs tidak cukup mumpuni untuk mengenali indikasi jika mengalami serangan, apalagi sampai kemudian memulihkan.

Sebenarnya pemerintah sudah melakukan sejumlah mitigasi, termasuk pembentukan Satgas Pemberantasan Judol. Salah satu tugasnya adalah memblokir situs-situs web yang terindikasi mengandung tautan judol tersebut. Namun efektivitasnya masih jauh panggang dari api. Dari total 5.159 situs judi yang terverifikasi dalam riset ini, hanya 11% yang berhasil diblokir.

Artinya, hampir 50% situs tersisipi judol tersebut masih bisa diakses secara bebas menggunakan penyedia layanan internet di Indonesia. Sisanya hanya tidak bisa diakses karena kesalahan peladen atau situs yang memang sudah mati sendiri, bukan karena tindakan tegas pemblokiran. Hal ini menunjukkan bahwa sistem benteng pertahanan digital kita masih memiliki celah keamanan sangat lebar.

Temuan tersebut membuka mata kita bahwa serangan injeksi judol tak sekadar iklan ilegal, tetapi juga tamparan terhadap keamanan siber Indonesia. Domain resmi negara justru disalahgunakan untuk mempromosikan kegiatan melawan hukum.

Rekomendasi

Tentu saja tidak mudah menjawab masifnya serangan judol, termasuk dalam bentuk penyisipan iklan dan tautan ke situs web pemerintah. Namun, berdasarkan temuan riset ini, terdapat sejumlah rekomendasi baik umum maupun teknis, untuk menjawab atau setidaknya mengurangi dampak buruk serangan tersebut.

Pertama, untuk mencegah penyebaran lebih luas, diperlukan audit keamanan digital secara menyeluruh, pembersihan sistematis terhadap tautan judol, serta penguatan kapasitas teknis pengelola situs pemerintah agar domain .go.id kembali menjadi simbol keandalan dan integritas informasi publik di ruang digital.

Pemerintah pusat bersama pengelola setiap situs web perlu menegakkan prinsip kesesuaian format dan membangun sistem pengawasan berlapis terhadap pembuatan subdomain baru. Langkah-langkah tersebut penting untuk memastikan bahwa domain pemerintah Indonesia tetap kredibel, terverifikasi, dan aman, sekaligus mencegah penyalahgunaan nama domain negara sebagai sarana serangan atau disinformasi di ruang digital.

Kedua, regulasi yang bersifat umum perlu diikuti dengan peraturan turunan, termasuk SOP, agar tata kelola situs web pemerintah bisa berjalan dengan lebih baik. Komdigi perlu mewajibkan pengelola semua situs web pemerintah untuk *mereview* situs secara berkala (misalnya, seminggu sekali) dan melaporkannya ke penanggung jawab SOP di Komdigi.

Ketiga, adanya penanggung jawab keamanan dengan tugas fokus pada keamanan, bukan malah fungsi teknologi informasi yang terlalu luas, juga akan menjawab tantangan jika ada serangan. Tidak hanya terkait judol, tetapi serangan dalam bentuk lain, seperti DDoS dan penggantian tampilan.

Penambahan sumber daya manusia secara kuantitas juga perlu diikuti dengan upaya terus menerus meningkatkan kapasitas, baik kesadaran, pengetahuan, maupun keterampilan. Hal-hal sederhana semacam mengingatkan secara terus menerus dan melaksanakan pelatihan secara rutin juga akan berguna untuk memperkuat benteng pertahanan pemerintah dalam memerangi judol tersebut.

Terakhir, secara teknis, lembaga pemerintah perlu memperkuat penggunaan CMS populer seperti Wordpress dengan tambahan fitur keamanan seperti *plugin*, mengaktifkan 2FA, dan selalu diperbarui ke versi terakhir. Sebagai alternatif, *programming framework* seperti Code Igniter atau Laravel, juga bisa menjadi pilihan untuk alasan keamanan.

Glosarium

Istilah	Penjelasan
Linguistic Obfuscation	Teknik pengaburan bahasa dengan cara mengubah ejaan, bentuk kata, atau fonetik agar tidak mudah dideteksi oleh sistem otomatis (misalnya togel -- toggel). Digunakan dalam dunia siber untuk menghindari filter atau algoritma deteksi konten terlarang.
Social Engineering Lexical Indicators	Ciri-ciri linguistik dalam teks yang dirancang untuk memanipulasi emosi pengguna, seperti rasa serakah atau penasaran, guna mendorong tindakan tertentu (klik, login, transfer).
Geo-tagging (Digital)	Pemberian tanda geografis atau lokasi pada data digital, termasuk domain atau server, untuk menunjukkan asal wilayah atau target regional dari suatu aktivitas daring.
Brand Spoofing	Strategi peniruan merek terkenal (misal: “Zeus”, “Vegas”) untuk meniru kredibilitas dan meyakinkan pengguna bahwa situs palsu tersebut adalah entitas resmi atau tepercaya.
Domain Generation Algorithm (DGA)	Algoritma yang secara otomatis menghasilkan ribuan nama domain acak dengan pola tertentu (misal kombinasi angka “88”, “303”, “365”), sering digunakan oleh botnet, malware, atau jaringan spam.
Clickbait Incentive	Bentuk iming-iming atau ajakan emosional dalam teks (“menang besar”, “hadiah langsung”, “bonus tanpa batas”) untuk menarik klik atau interaksi tanpa dasar fakta yang jelas.
Lexical Classifier	Sistem atau algoritma yang mengklasifikasikan teks berdasarkan pola kata atau istilah, sering digunakan dalam deteksi konten berisiko seperti judi online atau phishing.
Teknik Jebakan (Deceptive Framing)	Strategi yang memberikan kesan teknis, profesional, atau ilmiah untuk menipu pengguna agar mempercayai suatu sistem palsu (contohnya klaim “RTP akurat”).

Istilah	Penjelasan
Institusionalisasi Identitas Digital Nasional	Proses formal pembentukan dan pengelolaan identitas digital negara (seperti domain .go.id) sebagai bagian dari infrastruktur hukum dan administrasi nasional.
Registry Nasional Domain	Lembaga resmi yang mengelola pendaftaran, administrasi, dan kebijakan domain tingkat nasional (contoh di Indonesia: PANDI).
Tata Kelola Digital (Digital Governance)	Sistem pengaturan, kebijakan, dan mekanisme kontrol pemerintah dalam mengelola sumber daya digital dan layanan publik daring.
Infrastruktur Digital Pemerintahan	Seluruh sistem teknis (server, domain, layanan web, keamanan) yang menopang komunikasi dan layanan publik berbasis internet di instansi pemerintah.
Legitimasi Digital (Digital Legitimacy)	Status resmi atau keabsahan suatu entitas di dunia maya, ditandai dengan kepemilikan domain, sertifikat keamanan, dan legalitas institusional.
Analisis Forensik Linguistik Domain	Pendekatan analisis yang menggabungkan linguistik, keamanan siber, dan OSINT untuk mengidentifikasi pola bahasa dan perilaku di nama domain berisiko.
Ekosistem Linguistik Digital	Kumpulan pola, kata, dan klaster semantik yang membentuk sistem komunikasi tertentu dalam ruang digital (misal: ekosistem kata judi online).
Obfuscation Pattern Recognition	Deteksi pola pengaburan bahasa atau ejaan yang disengaja dengan tujuan menghindari sistem keamanan.
Inaktivitas Digital	Kondisi di mana domain atau situs tidak lagi berfungsi, tidak merespons, atau kehilangan server aktif karena kelalaian, kadaluarsa, atau pembubaran lembaga.
Autentikasi Sistem (Token / Signature Validation)	Proses verifikasi kredensial digital (token, tanda tangan elektronik, atau API key) untuk memastikan pengguna dan server adalah entitas sah.
SSL/TLS Handshake Failure	Kegagalan pada tahap awal negosiasi koneksi aman (HTTPS), menandakan sertifikat tidak valid atau konfigurasi keamanan yang salah.
Keberlanjutan Infrastruktur Digital	Kemampuan sistem pemerintahan digital (domain, server, aplikasi) untuk tetap berfungsi, diperbarui, dan aman dalam jangka panjang.



SAFEnet