BRANDEFENSE COUNTRY REPORT · INDONESIA 2026

Brandefense: Laporan Lanskap Ancaman Siber Indonesia 2026

Sinyal paparan, klaim yang diperselisihkan, dan pertahanan dengan tanggung jawab yang jelas

Odin by Brandefense
Periode pengamatan: 1 Januari-22 November 2026
Versi 1.0 · Edisi Riset Publik · TLP:CLEAR · 8-22 November 2026

101/250
Domain yang dinilai dengan kredensial diiklankan untuk dijual saat diperiksa

18
Berkas kasus dengan status bukti berbeda

28
Label kelompok pemerasan dalam Ransompedia

90
Hari untuk peningkatan bertahap, bukan penundaan ancaman aktif

DAFTAR ISI

Daftar isi

Translated with AI

Edisi ini diterjemahkan dengan AI dari naskah utama bahasa Inggris. Jika terdapat perbedaan, edisi bahasa Inggris yang berlaku.

01	Ringkasan eksekutif	06
	Peta laporan	11
02	Konteks digital	12
03	Paparan organisasi terpilih	17
04	Bukti dark web	27
05	Keputusan per sektor	57
06	Gangguan dan penilaian klaim	63
07	Pelaku ancaman dan hubungan	69
08	Ekonomi penipuan	84
09	Perbankan dan jasa keuangan	89
10	Respons regulasi	95
11	Prospek bersyarat	101
12	Rencana tindakan dengan tanggung jawab yang jelas	105
	Lampiran	112
A	Lampiran A. Cakupan dan batas bukti	113
B	Lampiran B. Daftar bukti yang disamarkan	116
C	Lampiran C. Catatan verifikasi sumber	118
D	Lampiran D. Glosarium	121

Dewan dan pimpinan eksekutif	01 10 11 12
CISO dan pemimpin penanganan insiden	01 04 06 07 12
Penanggung jawab identitas dan aplikasi	03 04 05 08 09
Penanggung jawab infrastruktur dan kesinambungan	02 03 05 06 12
Privasi, hukum, dan komunikasi	04 06 09 10
Tim kejahatan keuangan dan operasional pelanggan	05 08 09 12

Tentang edisi ini

Diterjemahkan dengan AI. Jika terdapat perbedaan, edisi bahasa Inggris yang berlaku.

Brandefense Country Report · Indonesia 2026

Riset dan penyusunan naskah dibantu AI. Naskah utama bahasa Inggris menjadi acuan bagi edisi terjemahan.

Periode pengamatan: 1 Januari hingga 22 November 2026. Periode terkini: 8 hingga 22 November 2026. Pengamatan dihimpun sebelum 22 November berakhir.

Bukti mengenai Indonesia mendukung keputusan terpisah untuk validasi akses, kesinambungan layanan, dan kesiapan notifikasi. Bukti tersebut juga membatasi kesimpulan yang dapat ditarik dari iklan dan tanggal publikasi.

Angka utama	Makna
101/250	Domain organisasi yang dinilai dengan kredensial diiklankan untuk dijual saat diperiksa
59/100	Angka utama Atlas nasional untuk portofolio terpilih
74	Pencantuman terkait pemerasan berlabel Indonesia di Ransompedia selama periode pengamatan
28	Label kelompok yang terkait dengan pencantuman tersebut
6	Pencantuman bertanggal dalam periode terkini
241/250	Domain kandidat terpilih dengan pengamatan pasif; sembilan tidak tersedia

Angka pencantuman menggambarkan pengamatan Ransompedia. Angka tersebut tidak membuktikan 74 insiden ransomware terkonfirmasi, 74 korban unik, atau 74 penyusupan yang berhasil. Portofolio terpilih tidak mewakili seluruh organisasi Indonesia. [S2][S3][S4]

Daftar isi dan jalur baca

Bab	Pertanyaan yang dijawab
1. Ringkasan eksekutif	Keputusan apa yang perlu didanai dan diwajibkan pimpinan sekarang?
2. Konteks digital	Ketergantungan apa yang membentuk dampak paparan?
3. Paparan organisasi terpilih	Apa yang dapat dibuktikan portofolio terpilih mengenai kontrol yang dapat diamati?
4. Bukti dark web	Klaim mana yang perlu divalidasi, dan hal apa yang belum dipastikan?
5. Keputusan per sektor	Bagaimana sinyal yang sama menimbulkan dampak operasional yang berbeda?
6. Gangguan dan penilaian klaim	Bagaimana tim pertahanan membedakan peringatan, gangguan layanan, dan klaim serangan?
7. Pelaku ancaman dan hubungan	Hubungan antarpelaku mana yang didukung oleh bukti tertentu?
8. Ekonomi penipuan	Mengapa akses, materi identitas, dan catatan pembayaran memerlukan respons berbeda?
9. Perbankan dan jasa keuangan	Bagaimana lembaga keuangan menggabungkan bukti transaksi, identitas, dan layanan?
10. Respons regulasi	Penerima, pemicu, dan tenggat apa yang berlaku?
11. Prospek bersyarat	Sinyal apa yang akan mengubah penilaian?
12. Rencana tindakan dengan tanggung jawab yang jelas	Siapa yang bertanggung jawab atas pekerjaan dalam 30, 60, dan 90 hari mendatang?
Lampiran A	Cakupan, populasi, dan istilah tingkat keyakinan
Lampiran B	Daftar kasus dan bukti yang telah disamarkan
Lampiran C	Sumber dan tanggal verifikasi
Lampiran D	Glosarium

Pimpinan dapat memulai dari Bab 1, 10, dan 12. Tim operasi keamanan dapat mengikuti Bab 4, 6, dan 7 menuju daftar bukti. Penanggung jawab identitas, infrastruktur, dan aplikasi dapat menggunakan Bab 3, 5, 8, dan 9.

Laporan ini membedakan publikasi yang diamati dari dugaan yang mendasarinya. Laporan juga memisahkan pengungkapan organisasi, keterangan penyelidikan resmi, dan riset vendor. Atribusi dari suatu sumber tetap merupakan penilaian sumber tersebut.

Label bukti	Hal yang didukung	Hal yang tidak otomatis didukung
Pengamatan sendiri	Unggahan, pencantuman, atau kondisi terukur terdapat dalam populasi yang dinyatakan	Akses yang diiklankan berfungsi atau pencurian telah terjadi
Klaim pelaku	Suatu persona mengiklankan dugaan atau kemampuan	Insiden terkonfirmasi, penjualan selesai, atau identitas operator diketahui
Keterangan resmi atau pengendali	Fakta tertentu yang dilaporkan otoritas atau organisasi	Seluruh dugaan penjual yang berkaitan dengan tema yang sama
Riset vendor	Aktivitas dan penafsiran yang dijelaskan penerbit yang disebutkan	Atribusi resmi Indonesia atau gambaran nasional yang lengkap
Inferensi analitis	Penafsiran yang dinyatakan untuk menghubungkan hal-hal yang didukung bukti	Pengamatan baru atau konfirmasi independen

Makna tanggal dipertahankan sepanjang laporan. Tanggal unggahan mencatat publikasi. Tanggal pencantuman mencatat pencantuman terkait pemerasan. Penemuan, notifikasi, aktivitas serangan, dan pemberitaan publik dapat terjadi pada hari yang berbeda.

BAB 01

Ringkasan eksekutif

01

PERTANYAAN BAB INI

Keputusan apa yang mengikuti bukti mengenai Indonesia tanpa menganggap klaim sebagai insiden terkonfirmasi?

74

Pencantuman terkait pemerasan yang diamati selama periode laporan

1.1 Enam temuan bagi pimpinan 08

1.2 Empat keputusan bagi pimpinan 08

1.3 Tahun ini dalam angka 09

1.4 Hal yang mengubah keputusan respons 10

1.5 Cara menggunakan laporan 10

BAB 01

Ringkasan eksekutif

RINGKASAN

Bukti mengenai Indonesia memerlukan tiga jalur respons: validasi akses yang diiklankan, kesiapan menghadapi gangguan layanan, dan kesiapan notifikasi. Ransompedia mencatat 74 pencantuman terkait pemerasan dengan 28 label kelompok. Kasus publik mencakup penyelidikan pencurian dana, akses platform pelanggan, dan penyalahgunaan situs. Riset vendor turut mencatat kampanye bertarget, dengan batas penting pada tanggal dan atribusi. Populasi ini tidak membentuk jumlah insiden nasional. Tetapkan penanggung jawab untuk memvalidasi akses aktif, melatih pemulihan, dan memelihara catatan insiden yang siap disampaikan kepada regulator.

1.1 Enam temuan bagi pimpinan

1. **Pencantuman terkait pemerasan mencakup beberapa sektor yang penting secara operasional.** Ransompedia mencatat 74 pencantuman berlabel Indonesia selama periode laporan. Energi dan industri ekstraktif mencakup 13, sedangkan jasa digital dan profesional mencakup 12. Angka tersebut merupakan kategori pencantuman, bukan kejadian kerugian terkonfirmasi. [S2]

1. **Penawaran akses terkini memerlukan bukti keadaan akun saat ini.** Unggahan 22 November mengiklankan akses VPN perguruan tinggi dan mengklaim hak administrator domain. Penawaran pada Oktober memuat klaim akses jarak jauh sektor pertanian. Kartu B03 dan B04 menampilkan iklan tersebut. Penanggung jawab identitas perlu memvalidasi akun, sesi, dan izin sebelum menentukan pembatasan. [S1]

1. **Kasus resmi menunjukkan beberapa jenis dampak.** Polisi menjelaskan kerugian transaksi dalam penyelidikan bank daerah dan kasus dana sekolah. Sumber lain membahas akses platform pelanggan, dugaan paparan data pegawai yang diperselisihkan, dan perubahan tampilan situs tanpa izin. Satuan dan status buktinya berbeda. Menjumlahkan catatan, akun, situs, dan uang dari kasus tersebut akan menghasilkan angka tanpa makna. [S35][S36][S40][S41][S44]

1. **Publikasi pada 2026 tidak membuktikan aktivitas pada 2026.** Laporan Amaranth-Dragon dari Check Point pada Februari menjelaskan operasi di Indonesia pada Agustus dan September 2025. Publikasi StrikeShark dari Kaspersky tidak memberikan tanggal penyusupan yang pasti dalam keterangan pendukungnya. Karena itu, laporan mempertahankan pembedaan antara aktivitas terdahulu dan aktivitas yang tanggalnya tidak diketahui. [S21][S43]

1. **Kesiapan pelaporan memiliki beberapa penghitungan waktu.** UU PDP menetapkan pemberitahuan tertulis dalam 3 × 24 jam ketika terjadi kegagalan pelindungan. Ketentuan IIV, OJK, dan BI dalam cakupannya memiliki penerima dan pemicu berbeda. Catatan insiden bersama harus mendukung kewajiban tersebut tanpa menggantikan penilaian hukum masing-masing. [S6][S12][S15][S18]

1. **Iklan kredensial terkini memerlukan validasi pada portofolio terpilih.** Dalam pengamatan paparan, 101 dari 250 domain organisasi yang dinilai memiliki kredensial diiklankan untuk dijual. Angka utama Atlas nasional adalah 59/100. Sinyal ini tidak membuktikan keabsahan akun aktif atau penyusupan terkonfirmasi. Tetapkan penanggung jawab pemeriksaan akun saat ini dan perangkat terkait. [S4]

1.2 Empat keputusan bagi pimpinan

Danai validasi identitas dan penyimpanan bukti. Wajibkan penanggung jawab identitas menentukan apakah akun yang diiklankan masih valid, siapa pemiliknya, dan apakah penanganan sebelumnya sudah mengatasinya. Simpan bukti yang mendasari setiap keputusan.

Minta bukti pemulihan dari penanggung jawab layanan. Minta hasil latihan pemulihan yang diamati, mencakup layanan bisnis, ketergantungan identitasnya, dan pemasok eksternal. Daftar cadangan saja tidak membuktikan keberhasilan pemulihan.

Setujui alur kerja notifikasi bersama. Penanggung jawab hukum, privasi, keamanan, dan bisnis perlu menyepakati cara memasukkan fakta ke dalam catatan insiden. Alur tersebut harus menyimpan waktu penemuan, perkiraan waktu kejadian, sistem terdampak, dan tanda terima pengiriman.

Pisahkan pelindungan pelanggan dari atribusi publik. Komunikasi dapat menjelaskan status layanan dan langkah pelindungan selama penyelidik menilai akses, cakupan data, dan tanggung jawab. Label pelaku yang tidak didukung bukti hanya memberi sedikit manfaat bagi pelindungan pelanggan yang perlu segera dilakukan.

1.3 Tahun ini dalam angka

101/250

Domain yang dinilai dengan kredensial diiklankan untuk dijual saat diperiksa

BUKAN BERARTI

Pelanggaran terkonfirmasi atau akun aktif

59/100

Angka utama Atlas nasional untuk portofolio terpilih

BUKAN BERARTI

Prevalensi nasional atau probabilitas insiden

332,251

Unggahan berlabel negara dalam populasi metadata

BUKAN BERARTI

Penargetan terverifikasi, unggahan relevan yang disimpan, atau insiden berbeda

74

Pencantuman Ransompedia bertanggal dalam periode laporan

BUKAN BERARTI

Insiden ransomware Indonesia yang terkonfirmasi

28

Label kelompok yang melekat pada pencantuman tersebut

BUKAN BERARTI

Jumlah organisasi kriminal independen yang terbukti

6

Pencantuman Ransompedia dalam periode terkini

BUKAN BERARTI

Seluruh insiden siber dari 8 hingga 22 November

241/250

Domain kandidat dengan pengamatan pasif

BUKAN BERARTI

Cakupan nasional atau penilaian organisasi

166/241

Domain dengan kebijakan DMARC quarantine/reject teramati

BUKAN BERARTI

Penerapan penuh pada pengiriman pesan atau bukti bahwa email diblokir

12

Pencantuman dalam jasa digital dan profesional

BUKAN BERARTI

Ukuran dampak lanjutan terhadap pelanggan pemasok

3 × 24 jam

Kewajiban pemberitahuan tertulis menurut UU PDP dalam keadaan yang disebutkan

BUKAN BERARTI

Pengganti universal untuk pelaporan sektoral

1 jam

Jangka waktu notifikasi awal siber BI dalam cakupan peraturannya

BUKAN BERARTI

Tenggat bagi setiap usaha Indonesia

Hasil pasif menggambarkan pengamatan pada 241 dari 250 domain kandidat. Cakupan setiap kontrol tidak membuktikan keberhasilan serangan atau prevalensi nasional. [S3][S4]

Enam pencantuman terkini melibatkan empat label: Panzer, N0n, INC Ransom, dan Pixelleaks. N0n dan INC Ransom masing-masing mencakup dua. Label lainnya masing-masing mencakup satu. Enam pencantuman tersebut merupakan bagian dari sembilan pencantuman yang diamati pada November, bersama tiga pencantuman bertanggal 1 hingga 7 November. Frekuensi publikasi maupun keberadaan label tidak membuktikan penyusupan atau enkripsi yang berhasil. [S2]

1.4 Hal yang mengubah keputusan respons

Peringatan perlu menyebutkan hal yang harus divalidasi. Untuk penawaran akses, hal tersebut berkaitan dengan akses saat ini. Untuk penawaran data, hal tersebut berkaitan dengan asal dan cakupannya. Untuk peringatan gangguan, hal tersebut berkaitan dengan dampak layanan dan kesiapan.

Akun aktif yang tervalidasi memerlukan respons berbeda dari akun yang sudah dinonaktifkan dalam kumpulan data yang beredar kembali. Keduanya perlu memiliki keputusan penanganan yang tercatat. Hanya keadaan pertama yang mendukung pembatasan segera berdasarkan akses saat ini.

Pencantuman dapat menjadi alasan menghubungi penanggung jawab insiden organisasi dan meninjau telemetri yang tersedia. Tanpa bukti tambahan, pencantuman tidak membuktikan jalur akses awal, eksekusi malware, enkripsi, atau pembayaran tebusan.

Disiplin yang sama berlaku bagi pelaporan resmi. Pengumuman polisi memberikan keterangan penyelidikan. Pemberitahuan pengendali mencatat hal yang diungkapkannya. Penyelidikan yang belum selesai tidak boleh berubah menjadi penetapan akhir kesalahan dalam ringkasan.

1.5 Cara menggunakan laporan

Bab sektoral menerjemahkan bukti menjadi pekerjaan bagi penanggung jawab tertentu. Bab pelaku mengaitkan hubungan dengan sumbernya. Bab hukum mempertahankan penerima dan waktu pelaporan. Rencana tindakan memberikan pemicu dan bukti penyelesaian untuk setiap tugas.

Lampiran A menjelaskan mengapa angka tetap dipisahkan. Lampiran B menghubungkan berkas kasus dan kartu. Lampiran C mencatat sumber yang digunakan, termasuk tanggal verifikasinya. Identitas mentah korban atau rincian kontaknya tidak ditampilkan secara publik.

TEMUAN UTAMA

01

Validasi akses saat ini sebelum menentukan pembatasan

02

Minta bukti pemulihan layanan dari penanggung jawab yang ditetapkan

03

Siapkan satu catatan fakta insiden untuk beberapa kewajiban notifikasi

Peta laporan

Pilih jalur berdasarkan keputusan yang menjadi tanggung jawab Anda. Setiap jalur bergerak dari pengamatan yang didukung bukti menuju langkah validasi dan hasil yang terdokumentasi.

Dewan dan pimpinan eksekutif	Kemampuan dan tanggung jawab apa yang memerlukan pendanaan?	Buka 1 10 11 12
CISO dan pemimpin penanganan insiden	Hal apa yang memerlukan validasi atau eskalasi?	Buka 1 4 6 7 12
Penanggung jawab identitas dan aplikasi	Akun, sesi, dan integrasi mana yang perlu diperiksa?	Buka 3 4 5 8 9
Penanggung jawab infrastruktur dan kesinambungan	Ketergantungan apa yang harus tetap berfungsi saat terjadi gangguan?	Buka 2 3 5 6 12
Privasi, hukum, dan komunikasi	Fakta apa yang mendukung notifikasi dan pernyataan publik?	Buka 4 6 9 10
Tim kejahatan keuangan dan operasional pelanggan	Sinyal transaksi atau identitas apa yang mendasari tindakan pelindungan?	Buka 5 8 9 12

Bab	Baca untuk memahami
1	Keputusan dan batas angka yang mendasari laporan
2	Pandangan layanan digital berdasarkan ketergantungannya
3	Batas pengukuran portofolio terpilih
4	Hal yang dapat dibuktikan oleh setiap klaim yang disimpan atau kasus publik
5	Perbedaan validasi dan dampak antar sektor
6	Mengapa imbauan, gangguan layanan, dan klaim serangan merupakan kejadian terpisah
7	Hubungan mana dalam peta pelaku yang memiliki bukti pendukung
8	Cara merespons klaim mengenai materi identitas dan pembayaran
9	Cara sektor keuangan menggabungkan kontrol akses, transaksi, dan kesinambungan
10	Cara mempertahankan cakupan, pemicu, dan tenggat hukum
11	Perubahan yang mendukung eskalasi atau penurunan eskalasi
12	Cara menugaskan dan menyelesaikan pekerjaan dengan bukti

BAB 02

Konteks digital

02

PERTANYAAN BAB INI

Ketergantungan digital apa yang membentuk dampak insiden akses atau ketersediaan?

3

Waktu yang berbeda: aktivitas, penemuan, dan publikasi

2.1 Acuan bertanggal untuk keputusan saat ini 13
2.2 Identitas menghubungkan beberapa dampak 14
2.3 Koordinasi pusat tidak menghapus tanggung jawab layanan 14
2.4 Infrastruktur bersama dapat meneruskan dampak tidak langsung 15
2.5 Pesan kesiapsiagaan perlu diterjemahkan menjadi pekerjaan operasional 15
2.6 Konteks menentukan dampak, bukan atribusi 15

BAB 02

Konteks digital

RINGKASAN

Ketergantungan digital menjadikan identitas, aplikasi, dan layanan bersama sebagai urusan operasional. Konteks harus mempertahankan tanggalnya: laporan Digital 2026 Indonesia diterbitkan pada akhir 2025 menggunakan pengamatan yang tersedia saat itu. Keterangan publik pada 2026 menunjukkan dampak berbeda dari platform pelanggan, sistem keuangan, situs, dan infrastruktur bersama. Keterangan tersebut tidak membuktikan satu tren serangan nasional. Petakan ketergantungan setiap layanan kritis dan uji keputusan yang mengikuti hilangnya akses atau ketersediaan.

2.1 Acuan bertanggal untuk keputusan saat ini

Laporan Digital 2026 Indonesia dari DataReportal diterbitkan pada 5 November 2025. Bagian pendukungnya menyebut pengamatan Oktober 2025 dan pengamatan lain pada akhir 2025 sebagai acuan terbaru yang tersedia. Judul laporan tidak boleh dianggap sebagai pengukuran pada batas waktu pengamatan ini. [S81]

Acuan akhir 2025	Angka	Satuan dan batas
Pengguna internet	230 juta	Pengguna pada acuan bertanggal tersebut
Penetrasi internet	80.5%	Proporsi penduduk pada acuan tersebut
Koneksi seluler	331 juta; 116% dari penduduk	Koneksi bukan orang unik, dan tidak semuanya dapat mengakses internet

Pengamatan ini diterbitkan pada November 2025. Angka tersebut bukan pengukuran pada batas pengamatan saat ini atau jumlah populasi terdampak. [S81]

Laporan ini menggunakan sumber tersebut untuk konteks konektivitas digital. Penggunaan internet, koneksi seluler, atau identitas platform tidak diubah menjadi perkiraan jumlah orang yang terdampak. Populasi terhubung dan populasi terdampak merupakan satuan berbeda.

Sebagai konteks pemantauan nasional terdahulu, BSSN melaporkan 403,990,813 anomali trafik pada 2023 dan 330,527,636 anomali trafik pada 2024. [S96][S97] Angka tahunan tersebut menghitung anomali trafik dalam cakupan pemantauan BSSN, bukan penyusupan terkonfirmasi atau korban unik. [S96][S97] Angka tersebut memberikan acuan pemantauan tahun ke tahun yang terbatas dan tidak dapat digabungkan dengan jumlah unggahan dark web, pencantuman pemerasan, atau pengamatan paparan portofolio pada 2026.

Pertanyaan operasionalnya adalah ketergantungan. Alur layanan pelanggan dapat bergantung pada pendaftaran, pemulihan identitas, pesan, pemrosesan pembayaran, dan aplikasi pemasok. Insiden dapat memengaruhi satu komponen sementara komponen lain tetap tersedia.

Peta ketergantungan perlu menunjukkan siapa yang dapat mengesahkan perubahan untuk pelindungan. Peta juga perlu menunjukkan siapa yang dapat menjelaskan dampak kepada pelanggan. Kedua tanggung jawab tidak harus dipegang tim yang sama, tetapi perlu menggunakan satu catatan fakta insiden.

2.2 Identitas menghubungkan beberapa dampak

Penyelidikan bank daerah membahas transaksi tanpa izin dan dugaan penyusupan sistem. Pengungkapan platform pelanggan membahas informasi terkait akun. Penyelidikan situs membahas akses yang dijual untuk penyalahgunaan konten. Masing-masing menghubungkan identitas dengan hasil operasional yang berbeda. [S36][S38][S44]

Pembedaan ini mengubah validasi. Akun administrator situs memerlukan peninjauan perubahan konten, jalur akses, dan riwayat penerapan sistem. Akun keuangan memerlukan bukti transaksi dan pelindungan pelanggan. Akun aplikasi memerlukan penilaian data dan fungsi yang dapat diaksesnya.

Kata sandi yang muncul dalam kumpulan data tidak dapat menjawab pertanyaan tersebut sendirian. Organisasi harus menentukan apakah akun ada dan masih aktif. Organisasi juga harus memastikan apakah sesi atau token terkait tetap berlaku setelah kata sandi diganti.

Penyelidikan juga perlu membedakan akses pegawai, pemasok, dan pelanggan. Alamat yang tampak seperti alamat perusahaan tidak membuktikan hubungan kepegawaian. Akun pemasok dapat menimbulkan ketergantungan tanpa membuktikan insiden di seluruh pemasok.

2.3 Koordinasi pusat tidak menghapus tanggung jawab layanan

Perpres 82/2022 menjelaskan tim tanggap insiden nasional, sektoral, dan organisasi untuk IIV. Peraturan tersebut menjadikan BSSN koordinator pelindungan serta memberikan tanggung jawab sektoral kepada kementerian atau regulator. Respons organisasi tetap menjadi bagian dari struktur itu. [S12][S13]

Koordinasi pusat membantu menetapkan jalur pelaporan dan bantuan. Koordinasi tersebut tidak menggantikan pemilik aset aplikasi atau keputusan pemulihan penanggung jawab layanan. Organisasi tetap perlu mengetahui identitas, sistem, dan pemasok yang mendukung layanan kritis.

Prinsip yang sama berlaku bagi pengawasan keuangan. Peraturan OJK 2026 tentang TI bank umum membahas tata kelola, manajemen risiko, pihak ketiga, dan pelindungan data. Kerangka BI membahas keamanan informasi dan ketahanan siber dalam cakupannya sendiri. [S16][S18]

Daftar layanan yang praktis perlu menghubungkan ketentuan tersebut dengan operasional. Daftar perlu menunjukkan layanan bisnis, pengendali datanya, penanggung jawab teknis, identitas berhak istimewa, ketergantungan pemasok, dan kontak pelaporan yang berlaku.

2.4 Infrastruktur bersama dapat meneruskan dampak tidak langsung

Komdigi melaporkan akses ke layanan pengembangan perangkat lunak terganggu sekitar empat jam pada 6 November. Alamat IP bersama masuk ke pemblokiran terkait malware. Akses pulih setelah alamat tersebut dikeluarkan. [S47]

Keterangan tersebut mendukung kejadian ketidaktersediaan akibat pemblokiran. Keterangan itu tidak mendukung adanya penyusupan ke platform pengembangan. Hal ini juga menunjukkan bahwa alamat bersama tidak selalu tepat sebagai pengganti identitas layanan.

Bagi tim pertahanan, keputusan yang relevan adalah perubahan dan pemulihan yang terkendali. Pemblokiran untuk pelindungan perlu memiliki penanggung jawab, penilaian ketergantungan bersama, dan jalur peninjauan mendesak. Jika memungkinkan, keputusan perlu menggunakan bukti khusus layanan.

Kesinambungan bisnis perlu mencakup ketergantungan identitas eksternal, pengembangan, pesan, dan dukungan. Usaha dapat kehilangan suatu alur kerja tanpa kehilangan kendali atas servernya sendiri. Karena itu, laporan membedakan respons serangan dari pemulihan layanan yang lebih luas.

2.5 Pesan kesiapsiagaan perlu diterjemahkan menjadi pekerjaan operasional

Pemberitahuan Komdigi pada 10 November meneruskan koordinasi dan kegiatan kesiapsiagaan BSSN. Keterangan tersebut menganjurkan pemantauan, pembaruan keamanan, langkah autentikasi, dan kesiapan pemulihan. Keterangan itu tidak mengonfirmasi bahwa setiap serangan yang diperingatkan telah terjadi. [S48][S49]

Respons yang berguna mengubah imbauan menjadi daftar singkat pemeriksaan dengan penanggung jawab. Penanggung jawab infrastruktur memastikan status pembaruan keamanan sistem yang dapat diakses dari internet. Penanggung jawab identitas memeriksa akses berhak istimewa. Penanggung jawab kesinambungan memverifikasi jalur pemulihan.

Pemimpin penanganan insiden mencatat pemicu pemeriksaan tersebut. Imbauan dapat mendasari peningkatan kesiapan meskipun klaim ancamannya belum terverifikasi. Hal ini menghindari pengabaian kesiapsiagaan sepenuhnya maupun pernyataan bahwa insiden telah terjadi tanpa bukti.

2.6 Konteks menentukan dampak, bukan atribusi

Sumber publik menjelaskan sektor dan ketergantungan yang berbeda. Jumlah anomali trafik BSSN pada 2023 dan 2024 juga mengukur volume pemantauan nasional, bukan satu tren insiden pada 2026. [S96][S97] Sumber tersebut tidak membuktikan bahwa setiap kejadian memiliki operator, motif, atau metode akses awal yang sama. Kesamaan sasaran dapat mencerminkan kesamaan peluang, bukan koordinasi.

Penilaian vendor mengenai keterkaitan dengan negara tetap diatribusikan kepada penerbitnya dalam Bab 7. Bahasa, pokok umpan, dan peringatan publik tidak secara mandiri membuktikan identitas operator.

Karena itu, laporan menggunakan konteks untuk menjelaskan dampak bisnis. Laporan tidak menyimpulkan penyebab politik suatu kejadian siber atau mengadopsi retorika pelaku ancaman. Keputusan operasional bergantung pada akses, dampak, dan bukti.

TEMUAN UTAMA

01

Tampilkan tanggal pengamatan acuan dengan jelas

02

Petakan ketergantungan identitas dan pemasok pada layanan kritis

03

Ubah pemberitahuan kesiapsiagaan menjadi pemeriksaan dengan penanggung jawab dan hasil tercatat

BAB 03

Paparan organisasi terpilih

PERTANYAAN BAB INI

Apa yang dapat dibuktikan portofolio domain terpilih tanpa mengklaim prevalensi nasional?

101/250

Domain yang dinilai dengan kredensial diiklankan untuk dijual saat diperiksa

3.1 Populasi dan penafsiran 18
3.2 Kondisi yang dapat diamati dan keputusan bisnis 18
3.3 Catatan paparan merupakan pemicu validasi 23
3.4 Sinyal sektoral yang diamati mempertahankan cakupannya 25
3.5 Validasi harus berakhir pada hasil tingkat layanan 25
3.6 Pertanyaan pimpinan mengenai portofolio 26

BAB 03

Paparan organisasi terpilih

RINGKASAN

Dari 250 domain organisasi yang dinilai, 101 memiliki kredensial diiklankan untuk dijual saat diperiksa. Angka utama Atlas nasional adalah 59/100. Portofolio mencakup sedikitnya 1,178,666 keterkaitan perangkat dan 6,353,372 keterkaitan catatan kredensial. Populasi ini bertumpang tindih dan tidak membuktikan penyusupan saat ini. Pengamatan pasif mencakup 241 domain, dengan cakupan TLS dan HTTP tersendiri. Validasi iklan terkini dan hubungan pegawai, lalu tutup pengecualian kontrol dengan bukti produksi.

3.1 Populasi dan penafsiran

Populasi	Satuan	Penafsiran
Portofolio kandidat terpilih	250 domain utama	Portofolio yang dipilih secara terarah untuk konteks tingkat organisasi
Pengamatan kontrol pasif	Domain yang dinilai untuk setiap kontrol	Kondisi yang diamati dalam cakupan yang dinyatakan
Iklan akses saat ini	Organisasi atau akun dalam pengamatan yang ditetapkan	Sinyal validasi dengan makna waktu tersendiri
Keterkaitan kredensial dan perangkat	Satuan catatan atau keterkaitan yang dinyatakan	Bukti yang memerlukan pemeriksaan akun dan kepemilikan
Kasus laporan publik	Berkas kasus dengan jenis bukti berbeda	Contoh dampak, bukan survei insiden yang representatif

Portofolio kandidat merupakan batas analisis. Portofolio itu bukan klaim bahwa 250 organisasi terbesar telah diukur secara lengkap. Domain dapat mewakili layanan, grup, anak perusahaan, atau lingkup operasional bersama. [S4]

Penyebut suatu kontrol perlu mengikuti catatan yang benar-benar dinilai. Pengamatan yang tidak tersedia tidak dapat diubah menjadi nol. Ketiadaan respons juga tidak membuktikan ketiadaan kontrol di seluruh organisasi.

Portofolio berisi 250 domain utama kandidat dalam sepuluh kelompok sektor gabungan. Setiap pengamatan pasif mempertahankan penyebut yang dinilainya sendiri. [S4]

3.2 Kondisi yang dapat diamati dan keputusan bisnis

Angka utama Atlas nasional adalah 59/100 untuk portofolio terpilih. Nilai lebih tinggi menunjukkan paparan teramati lebih besar. Angka ini bukan persentase pelanggaran, probabilitas insiden, atau sertifikasi kontrol. Hanya angka utama nasional yang disajikan. [S4]

59/100

Angka utama Atlas nasional untuk portofolio terpilih berisi 250 domain

101/250

Domain organisasi yang dinilai dengan kredensial diiklankan untuk dijual saat diperiksa

Data paparan Atlas dibaca pada 22 November 2026. Pengamatan perangkat dan kredensial dapat mencakup catatan lama serta hubungan di luar tenaga kerja organisasi. Penilaian tidak membuktikan bahwa catatan tersebut pertama kali muncul selama periode laporan. [S4]

Pengamatan pasif email dan web menggambarkan kondisi pada saat penilaian. Catatan kebijakan dapat mendukung pernyataan mengenai catatan tersebut. Catatan itu tidak dapat membuktikan apakah pesan phishing mencapai pengguna atau menyebabkan kompromi akun. [S3]

Penanggung jawab kontrol perlu memvalidasi hasil terhadap layanan produksi. Domain dapat mewarisi pengaturan, menggunakan layanan pengiriman terpisah, atau berada dalam migrasi yang direncanakan. Penjelasan tersebut memerlukan bukti sebelum temuan ditutup.

Hasil yang berguna adalah daftar pengecualian dengan penanggung jawab. Setiap pengecualian perlu memiliki penanggung jawab layanan, dampak, dan uji penyelesaian. Catatan perubahan baru ditutup setelah kondisi hasilnya diperiksa.

Pengamatan tersedia untuk 241 dari 250 domain kandidat terpilih pada 22 November. Sembilan domain tidak tersedia. Ini merupakan pengamatan tingkat domain, bukan jumlah organisasi yang diverifikasi secara independen. [S3][S4]

Definisi kontrol dan batas pengamatan ini terdapat dalam Lampiran D.

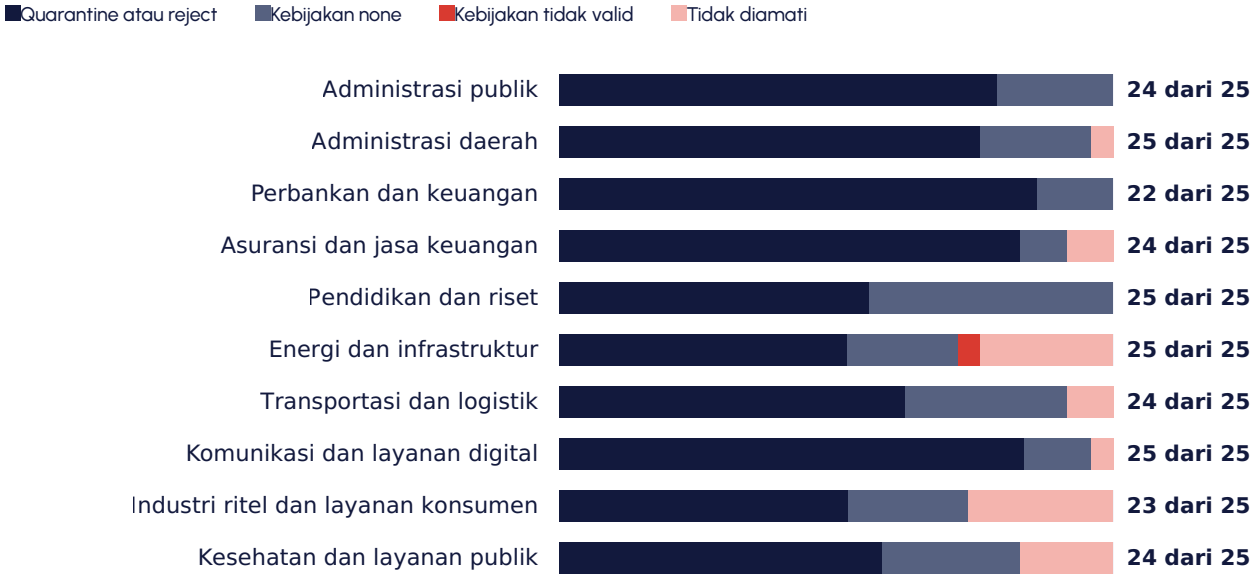
Pengamatan email atau DNS	Jumlah	Penyebut
Kebijakan DMARC quarantine/reject teramati	166	241
Kebijakan DMARC none teramati	52	241
Kebijakan DMARC tidak valid	1	241
Kebijakan DMARC tidak teramati	22	241
Catatan SPF teramati	230	241

Pengamatan email atau DNS	Jumlah	Penyebut
Catatan terkait DKIM teramati	169	241
Bukti delegasi DNSSEC teramati	33	241

Jumlah DMARC quarantine/reject mencakup 63 kebijakan reject dan 103 quarantine. Keberadaan kebijakan tidak membuktikan penerapan penuh pada pengiriman pesan, termasuk penanganan setiap pesan. [S3]

Catatan SPF dan catatan terkait DKIM tidak memvalidasi pengiriman pesan atau hasil autentikasi. Pengamatan terkait DKIM atau DNSSEC yang tidak ada di sini tidak membuktikan ketiadaan di seluruh layanan. Setiap penanggung jawab perlu memastikan konfigurasi produksi yang relevan.

Pengamatan kebijakan DMARC bervariasi di antara portofolio sektor terpilih



Sumber: pengamatan pasif untuk 241 dari 250 domain kandidat terpilih, 22 November 2026 [S3]. Penyebut sektoral adalah domain yang diamati. Keberadaan kebijakan tidak membuktikan penegakan pesan; pengamatan yang tidak tersedia tidak membuktikan ketiadaan kontrol.

Sektor	Domain teramati	DMARC quarantine/ reject	SPF	Terkait DKIM	Bukti DNSSEC
Administrasi publik	24	19	23	13	12
Administrasi daerah	25	19	25	14	5
Perbankan dan keuangan	22	19	22	13	4
Asuransi dan jasa keuangan	24	20	24	19	3
Pendidikan dan riset	25	14	25	23	3

Sektor	Domain teramati	DMARC quarantine/ reject	SPF	Terkait DKIM	Bukti DNSSEC
Energi dan infra-struktur	25	13	23	15	0
Transportasi dan logistik	24	15	24	20	1
Komunikasi dan layanan digital	25	21	23	21	4
Industri, ritel, dan layanan konsu-men	23	12	20	13	0
Kesehatan dan la-yanan publik	24	14	21	18	1

Setiap sektor berisi 25 domain kandidat terpilih. Kolom domain teramati merupakan penyebut untuk jumlah catatan email dan DNS pada sektor tersebut. Jumlah menggambarkan catatan teramati, bukan penilaian sektor atau keberhasilan phishing. [S3][S4]

Status TLS	Jumlah	Penyebut
Valid	205	241
Tidak valid	13	241
Tidak tersedia	23	241

Sektor	TLS valid	TLS tidak valid	TLS tidak tersedia	Penyebut
Administrasi publik	18	1	5	24
Administrasi daerah	20	3	2	25
Perbankan dan keu-angan	18	1	3	22
Asuransi dan jasa keu-angan	20	1	3	24
Pendidikan dan riset	21	1	3	25
Energi dan infrastruk-tur	24	0	1	25
Transportasi dan logis-tik	23	0	1	24
Komunikasi dan layan-an digital	23	1	1	25

Sektor	TLS valid	TLS tidak valid	TLS tidak tersedia	Penyebut
Industri, ritel, dan layanan konsumen	17	5	1	23
Kesehatan dan layanan publik	21	0	3	24

Status TLS dan cakupan HTTP terpisah. Pengamatan HTTP tersedia untuk 154 dari 241 domain teramati. Jumlah header di bawah menggunakan 154, bukan 241, sebagai penyebutnya. [S3]

Pengamatan header	Jumlah	Penyebut
HSTS	103	154
Content Security Policy	67	154
Header pelindungan frame	93	154
Header pelindungan jenis konten	91	154

Sektor	Pengamatan HTTP	HSTS	CSP	Frame	Jenis konten
Administrasi publik	11	9	6	7	9
Administrasi daerah	17	9	4	9	7
Perbankan dan keuangan	10	9	7	5	8
Asuransi dan jasa keuangan	12	11	7	10	10
Pendidikan dan riset	16	9	7	12	10
Energi dan infrastruktur	20	12	10	11	12
Transportasi dan logistik	15	9	3	7	7
Komunikasi dan layanan digital	18	13	9	13	10
Industri, ritel, dan layanan konsumen	17	11	9	12	11
Kesehatan dan layanan publik	18	11	5	7	7

Jumlah pengamatan HTTP setiap sektor merupakan penyebut untuk jumlah header pada sektor tersebut. Pengamatan HTTP yang tidak tersedia tidak membuktikan ketiadaan header di seluruh layanan. Kondisi ini tidak membuktikan eksploitasi, insiden data, atau efektivitas kontrol. [S3]

3.3 Catatan paparan merupakan pemicu validasi

Catatan kredensial lama mendukung respons berbeda dari akun berhak istimewa yang sedang diiklankan. Yang pertama memerlukan pemeriksaan kebaruan dan penanganan sebelumnya. Yang kedua memerlukan validasi mendesak atas dugaan akses saat ini.

Keterkaitan perangkat juga memerlukan penafsiran. Keterkaitan dapat melibatkan pegawai, kontraktor, pelanggan, atau hubungan lain. Laporan tidak menyimpulkan peran seseorang hanya dari rangkaian teks domain.

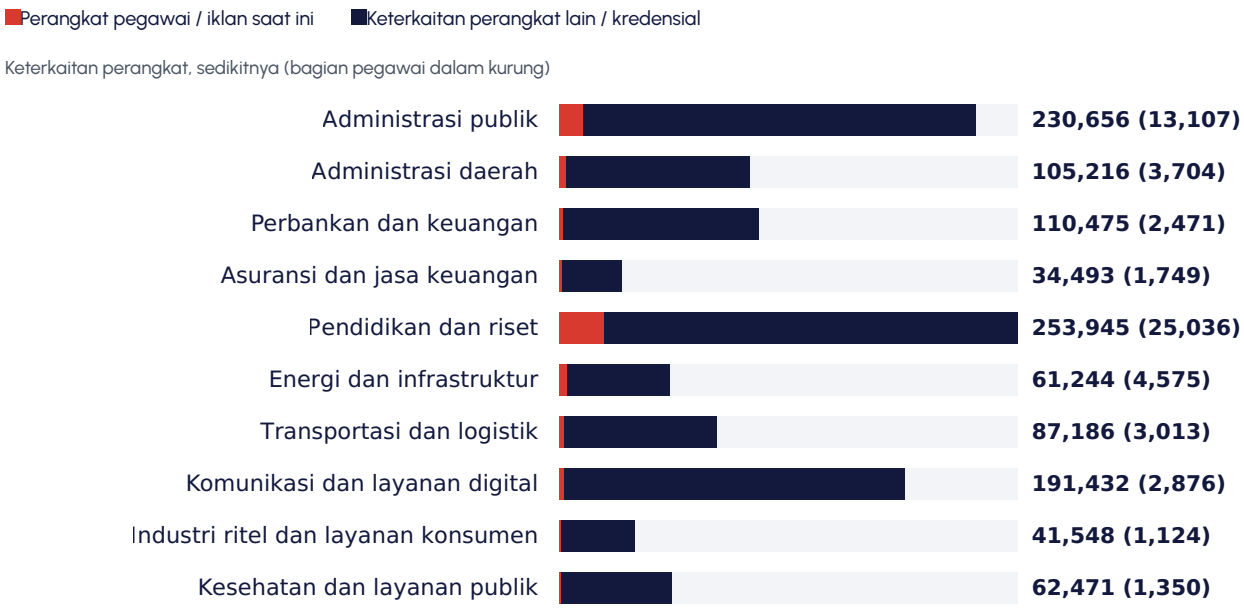
Saat memvalidasi paparan, penanggung jawab identitas perlu mencatat keadaan akun pada waktu keputusan. Catatan perlu membedakan akun nonaktif, akun yang diubah, akun aktif, dan hasil yang belum diketahui. Bukti keadaan akun saat ini harus mendahului pengaturan ulang yang mengganggu operasi.

Dari 250 domain organisasi yang dinilai, 101 memiliki kredensial diiklankan untuk dijual saat diperiksa. Keterkaitan perangkat teramati pada 243 domain; 234 memiliki keterkaitan perangkat pegawai, dan 246 memiliki keterkaitan catatan kredensial. Sinyal yang bertumpang tindih ini bukan jumlah penyusupan terkonfirmasi. [S4]

Portofolio mencakup sedikitnya 1,178,666 keterkaitan perangkat, termasuk 59,005 keterkaitan perangkat pegawai. Keterkaitan catatan kredensial berjumlah 6,353,372. Pengamatan juga mencatat 1,516 keterkaitan dokumen dan 32,205 pengamatan domain serupa dalam 30 hari sebelumnya. [S4]

Keterkaitan perangkat pegawai merupakan bagian dari tampilan perangkat dan tidak boleh ditambahkan padanya. Keterkaitan perangkat dapat bertumpang tindih antardomain serta mencakup hubungan pelanggan atau hubungan lain. Catatan kredensial bukan orang unik, akun aktif, atau pencurian terkonfirmasi.

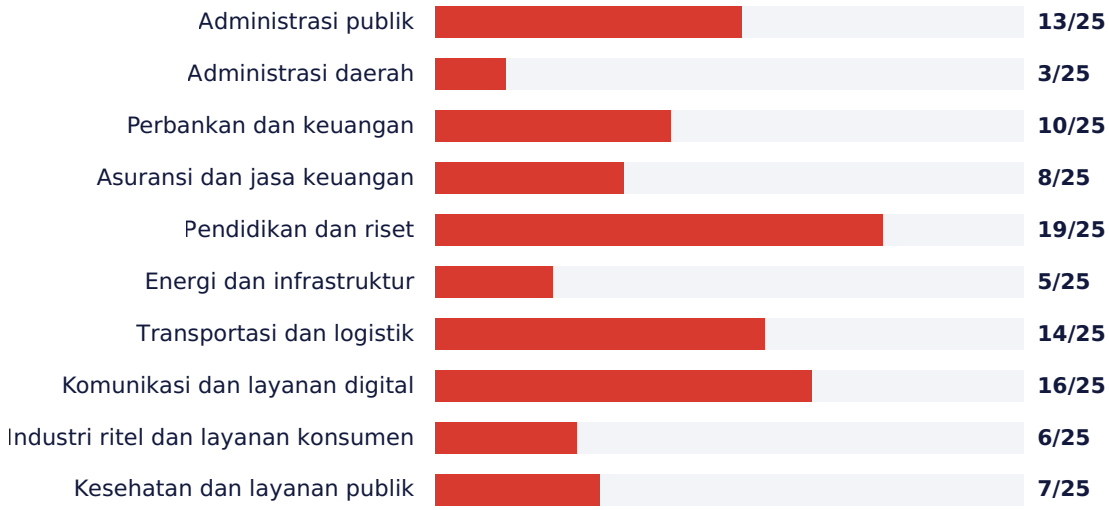
Populasi perangkat dan kredensial sektor berbeda dalam skala dan makna



Keterkaitan catatan kredensial (skala terpisah)



Iklan kredensial saat ini menurut sektor (koral)



Sumber: pengamatan paparan Brandefense Atlas untuk 250 domain yang dinilai, 22 November 2026 [S4]. Keterkaitan perangkat merupakan batas minimum; perangkat pegawai adalah bagian darinya. Catatan kredensial bukan orang unik, akun aktif, atau pencurian terkonfirmasi.

Sektor	Domain	Perangkat, sedikitnya	Perangkat pegawai	Catatan kredensial	Domain beriklan saat ini	Dokumen	Domain serupa, 30 hari
Administrasi publik	25	230,656	13,107	901,931	13	252	359
Administrasi daerah	25	105,216	3,704	294,095	3	45	167
Perbankan dan keuangan	25	110,475	2,471	355,135	10	395	5,072
Asuransi dan jasa keuangan	25	34,493	1,749	155,092	8	55	6,110

Sektor	Domain	Perangkat, sedikitnya	Perangkat pegawai	Catatan kredensial	Domain beriklan saat ini	Dokumen	Domain serupa, 30 hari
Pendidikan dan riset	25	253,945	25,036	3,527,006	19	195	3,751
Energi dan infrastruktur	25	61,244	4,575	375,178	5	158	1,508
Transportasi dan logistik	25	87,186	3,013	237,992	14	106	2,854
Komunikasi dan layanan digital	25	191,432	2,876	249,505	16	220	2,214
Industri ritel dan layanan konsumen	25	41,548	1,124	169,208	6	39	9,046
Kesehatan dan layanan publik	25	62,471	1,350	88,230	7	51	1,124
Total	250	1,178,666	59,005	6,353,372	101	1,516	32,205

Setiap sektor berisi 25 domain yang dinilai. Jumlah mendukung gambaran anonim portofolio terpilih ini. Dokumen memerlukan pemeriksaan kepemilikan dan sensitivitas; kemiripan nama saja tidak membuktikan penyamaran berba-
haya. Jumlah perangkat merupakan batas minimum, dan jumlah ini tidak menunjukkan prevalensi nasional. [S4]

3.4 Sinyal sektoral yang diamati mempertahankan cakupannya

Pembahasan sektor menggunakan kondisi yang dapat diamati dan bukti kasus yang disajikan di sini. Peringkat Atlas sektoral atau kelompok tidak dilaporkan. Jumlah sektoral tidak memperkirakan prevalensi nasional.

Pengamatan paparan terkait domain tidak memvalidasi iklan akses yang disimpan. Iklan tidak membuktikan bahwa catatan lama masih aktif. Setiap jenis bukti mempertahankan populasi dan tugas validasinya sendiri.

3.5 Validasi harus berakhir pada hasil tingkat layanan

Untuk pengecualian kebijakan email, penyelesaian berarti pemilik domain telah mengonfirmasi kebijakan yang dimaksud dan catatan yang dinilai mencerminkannya. Permintaan perubahan tanpa pengamatan hasil belum lengkap.

Untuk akun yang diiklankan, penyelesaian berarti penanggung jawab identitas telah memastikan status akun dan meninjau aktivitas yang relevan. Pembatasan mengikuti risiko saat ini yang terkonfirmasi. Penanggung jawab insiden mencatat alasan perlunya tindakan yang lebih luas atau alasan tidak diperlukannya tindakan tersebut.

Untuk sinyal domain serupa atau dokumen, penyelesaian berarti penanggung jawab bisnis telah menilai hubungan dan dampaknya. Kemiripan nama saja tidak membuktikan penyamaran identitas. Penyebutan saja tidak membuktikan hilangnya data internal.

3.6 Pertanyaan pimpinan mengenai portofolio

Dewan perlu menanyakan apakah layanan kritis memiliki penanggung jawab untuk paparan eksternal. Dewan juga perlu menanyakan kecepatan validasi klaim akun dan cara membuktikan bahwa perubahan kontrol telah diterapkan pada layanan produksi.

Angka utama nasional membantu menentukan prioritas portofolio. Iklan terkini dan hubungan perangkat pegawai tetap memerlukan pemilik aset, pemeriksaan akun saat ini, dan hasil validasi tercatat. Pengamatan kontrol pasif memerlukan pengujian penyelesaian pada tingkat layanan tersendiri.

Karena itu, bab portofolio perlu dibaca sebagai alat bantu keputusan. Nilainya terletak pada hubungan antara pengamatan terbatas, tindakan yang sebanding, dan hasil terdokumentasi.

TEMUAN UTAMA

01

Pertahankan penyebut yang dinilai untuk setiap kontrol

02

Validasi status akun sebelum respons yang mengganggu operasi

03

Tutup temuan dengan bukti produksi dari penanggung jawab layanan

BAB 04

Bukti dark web

04

PERTANYAAN BAB INI

Pengamatan mana yang mendasari penyelidikan, dan klaim mana yang belum dipastikan?

18

Berkas kasus dengan status bukti berbeda

4.1 Populasi unggahan yang disimpan 28
4.2 Dari klaim menuju keputusan 31
4.3 Sembilan berkas kasus dari korpus yang disimpan 32
4.4 Enam berkas kasus eksternal 42
4.5 Penawaran akses dan pemerasan tambahan 49
4.6 Data berulang tidak membuktikan penyusupan berulang 52
4.7 Periode terkini memiliki batas tersendiri 52
4.8 Tema tambahan mempertahankan batas yang lebih sempit 53
4.9 Pengamatan tambahan mengenai layanan dan penyampaian ulang klaim 55

BAB 04

Bukti dark web

RINGKASAN

Unggahan membuktikan bahwa klaim dipublikasikan. Unggahan tidak membuktikan akses berfungsi, penjualan selesai, atau penyusupan baru. Keterangan resmi dan pengendali mendukung hal yang lebih kuat, tetapi masing-masing tetap memiliki batas. Berkas kasus berikut memisahkan tanggal publikasi, aktivitas, pengungkapan, dan tindak lanjut. Angkanya tidak dapat dijumlahkan menjadi angka nasional. Untuk setiap dugaan relevan, tentukan hal yang perlu divalidasi, penanggung jawab yang dapat mengujinya, dan bukti yang akan menutup keputusan.

4.1 Populasi unggahan yang disimpan

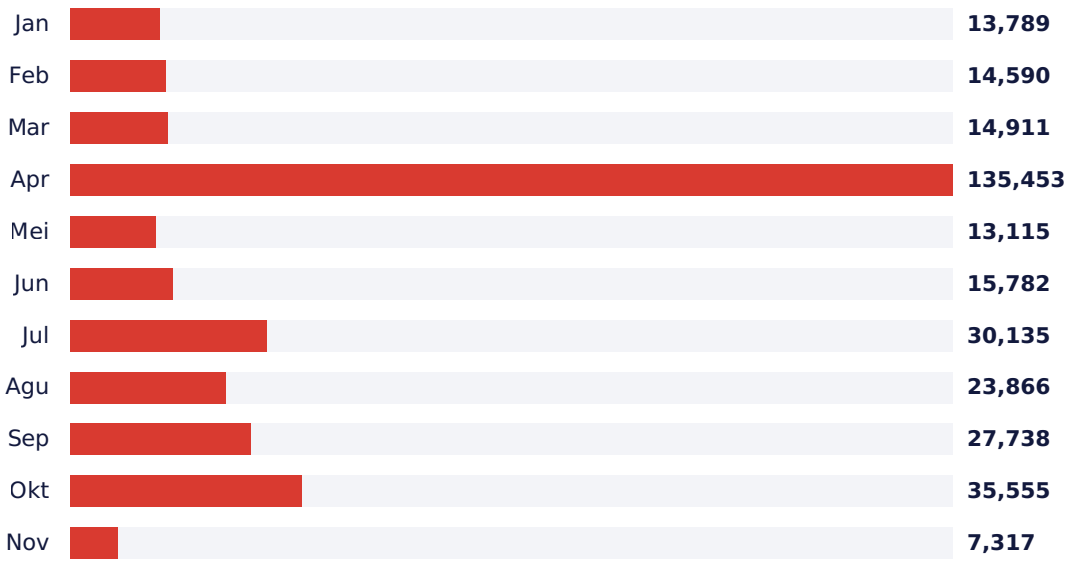
Pengamatan Brandefense Blackhole dan pencantuman Ransompedia menjawab pertanyaan berbeda. Unggahan menunjukkan publikasi persona dalam korpus yang disimpan. Pencantuman terkait pemerasan menunjukkan populasi pencantuman bertanggal. Keterangan insiden publik dapat menjelaskan kejadian yang tidak muncul dalam kedua populasi. [S1][S2]

Label negara tidak membuktikan sasaran berada di negara tersebut. Penjual dapat menggunakan kembali data lama, mengulang iklan, atau menjelaskan infrastruktur di luar kendali korban yang diklaim. Laporan mempertahankan alternatif tersebut.

Karena itu, korpus yang disimpan tidak disajikan sebagai sensus insiden Indonesia. Jumlah populasi yang pasti, jika tersedia, tetap dipisahkan dari kartu bukti dan berkas kasus terpilih. Beberapa pesan dapat menyangkut satu dugaan.

Jumlah metadata berlabel negara adalah 332,251 unggahan. Korpus yang disimpan berisi 19,814 unggahan berbeda dalam periode laporan. Cakupan kedua populasi berbeda. Korpus yang disimpan bukan pecahan yang dapat digunakan untuk memperkirakan relevansi nasional. [S1]

April memiliki volume metadata berlabel negara terbesar



Sumber: Brandefense Blackhole, 332,251 unggahan metadata berlabel Indonesia, 1 Januari–22 November 2026; hari terakhir parsial [S1]. Terpisah dari 19,814 unggahan yang disimpan; bukan jumlah penargetan atau insiden.

Bulan	Unggahan berlabel negara
Januari	13,789
Februari	14,590
Maret	14,911
April	135,453
Mei	13,115
Juni	15,782
Juli	30,135
Agustus	23,866
September	27,738
Oktober	35,555
November hingga pengambilan data	7,317

Nilai April merupakan pengamatan volume publikasi. Nilai itu tidak membuktikan lonjakan penargetan atau penyusupan berhasil. November hanya mencakup hingga pengambilan data pada 22 November dan tidak dapat dibandingkan dengan bulan lengkap sebagai hasil sebulan penuh. [S1]

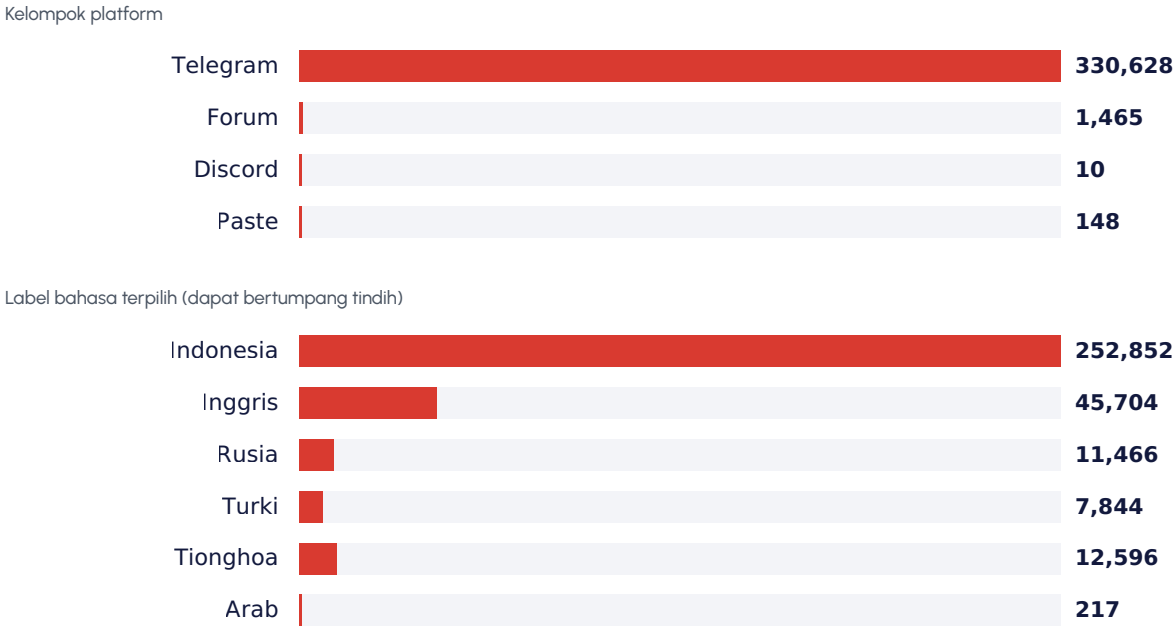
Platform	Kelompok label negara	Korpus yang disimpan
Telegram	330,628	17,340
Forum	1,465	2,466
Paste	148	7
Discord	10	1

Tabel hanya menampilkan sarana dengan pengamatan.

Kelompok platform dan jumlah berlabel negara sama-sama berjumlah 332,251 pada 22 November 2026. Keselarasan ini berkaitan dengan metadata, bukan bukti penargetan atau insiden terkonfirmasi. [S1]

Jumlah forum yang disimpan bukan bagian dari kelompok forum berlabel negara. Populasi memiliki cakupan berbeda. Jumlahnya tidak boleh digabungkan atau digunakan untuk menghitung porsi insiden nasional.

Kelompok platform dan bahasa menggambarkan keterlihatan metadata



Sumber: Brandefense Blackhole, 332,251 unggahan metadata berlabel Indonesia, 1 Januari–22 November 2026; hari terakhir parsial [S1]. Terpisah dari 19,814 unggahan yang disimpan; bukan jumlah penargetan atau insiden.

Label bahasa terpilih	Unggahan berlabel
Indonesia	252,852
Inggris	45,704
Bahasa Tionghoa	12,596
Rusia	11,466
Turki	7,844
Arab	217

Label bahasa dapat bertumpang tindih, dan tabel menampilkan enam bahasa terpilih. Tabel bukan pembagian yang saling terpisah. Bahasa tidak mengidentifikasi kewarganegaraan operator atau membuktikan pihak yang disasar. [S1]

Populasi terkini berlabel negara memuat 5,443 unggahan: 5,395 Telegram, 47 forum, dan satu Discord. Ini merupakan unggahan, bukan insiden berbeda. Penawaran terkini mengenai perguruan tinggi dan materi identitas menggambarkan perlunya validasi keadaan saat ini. [S1]

4.2 Dari klaim menuju keputusan

Penyelidikan yang berguna dimulai dari kemampuan yang diiklankan. "Data", "administrator", dan "akses" tidak menyiratkan izin yang sama. Penanggung jawab layanan perlu menentukan hal yang relevan bagi risiko organisasi saat ini.

Untuk penawaran data, pertanyaan relevan menyangkut asal, periode, dan apakah materi memuat informasi organisasi. Untuk penawaran akses, pertanyaan relevan menyangkut akun yang ada, keabsahan saat ini, dan izin yang diberikannya.

Sampel yang tampak kredibel tidak memastikan semua hal. Sampel lama dapat mendukung kepemilikan data sambil membiarkan akses saat ini belum terbukti. Tangkapan layar dapat menunjukkan sesi tanpa membuktikan durasi, asal, atau cakupannya.

Respons perlu mempertahankan perbedaan tersebut. Peringatan identitas perlu mencapai penanggung jawab identitas. Dugaan data pelanggan perlu mencapai tim privasi dan insiden pengendali. Pencantuman terkait pemerasan perlu mengaktifkan jalur peninjauan yang telah ditetapkan.

Keadaan bukti	Pertanyaan segera	Penanggung jawab	Bukti penyelesaian
Klaim akun atau akses berhak istimewa	Apakah akun yang dikelola saat ini valid, dan apa yang dapat dijangkaunya?	Penanggung jawab identitas dan layanan	Keadaan akun, peninjauan sesi, dan cakupan akses
Dugaan penjualan data	Apakah materi cocok dengan data yang dikelola, dan berasal dari periode apa?	Pemilik data dan penanggung jawab privasi	Penilaian asal dan cakupan data yang terbatas
Pencantuman terkait pemerasan	Apakah ada bukti tambahan mengenai akses, enkripsi, atau pengambilan data keluar?	Pemimpin penanganan insiden	Peninjauan telemetri dan keputusan penanganan insiden terdokumentasi
Klaim gangguan	Apakah layanan mengalami dampak yang sesuai dengan klaim?	Penanggung jawab layanan dan jaringan	Bukti ketersediaan dan permintaan beserta penanda waktu
Peredaran kembali materi lama	Apakah materi sudah ditangani atau diungkap?	Penanggung jawab catatan insiden dan privasi	Hubungan dengan kasus terdahulu dan validasi risiko yang tersisa

4.3 Sembilan berkas kasus dari korpus yang disimpan

A

KASUS A

Akses terkait perbankan diiklankan sebagai akses saat ini

Kartu bukti B01 | 17 Okt 2026 | Iklan yang disimpan | Kelompok perbankan

Klaim belum terverifikasi

KLAIM

Unggahan 17 Oktober menawarkan dugaan akses backend mobile banking, basis data API promosi, serta informasi pelanggan atau administrator. Penjual menyebut akses masih berlaku. [S1]

KRONOLOGI

Iklan yang disimpan bertanggal 17 Oktober 2026. Pernyataannya mengenai akses aktif merupakan klaim kondisi saat itu, bukan pengamatan akses produksi yang terverifikasi.

HAL YANG DIBUKTIKAN

Iklan menawarkan akses dan mengusulkan verifikasi pembeli. Iklan menjelaskan sistem perbankan dan promosi sebagai unsur berbeda. Publikasi dan penawaran komersial didukung bukti.

ALTERNATIF

Deskripsi dapat mencampurkan deskripsi layanan, infrastruktur promosi, dan paparan pelanggan. Materi yang beredar ulang, pembesaran klaim, atau pemalsuan tetap mungkin.

BATAS	Akses saat ini, keaslian data pelanggan, izin, cakupan seluruh bank, dan transaksi selesai belum dipastikan. Unggahan tidak membuktikan insiden perbankan terkonfirmasi.
RESPONS	Penanggung jawab layanan dan identitas perlu memvalidasi batas autentikasi yang diduga serta meninjau akses relevan. Respons yang memuat informasi sensitif dan alur pemulihan akun perlu ditinjau jika hubungan layanan telah dibuktikan.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B01 17 Okt 2026

updap Iklan yang disimpan Forum Inggris

TEKS ASLI

This is not historical data. This is live production access right now.

TERJEMAHAN

Ini bukan data lama. Ini akses produksi yang masih aktif sekarang.

Catatan. Pernyataan di bawah merupakan klaim penjual, bukan pengamatan akses yang terverifikasi.

Hal yang dibuktikan
Iklan yang disimpan menawarkan akses dan verifikasi pembeli yang melibatkan sistem perbankan dan promosi.

Belum dipastikan
Akses saat ini, keaslian data pelanggan, izin, cakupan seluruh bank, dan penjualan selesai belum dipastikan.

B

KASUS B

Penawaran layanan pendapatan mencampurkan akses dan populasi catatan

Klaim belum terverifikasi

Kartu bukti B02 · 31 Okt 2026 · Iklan yang disimpan · Layanan pendapatan sektor publik

KLAIM	Iklan 31 Oktober menyangkut layanan pendapatan sektor publik. Iklan mengklaim akses berhak istimewa serta menawarkan sekitar 10.5 juta catatan pengajuan, 3.4 juta pengenal wajib pajak, dan sekitar 23,000 kasus pengembalian dana seharga $3,500. [S1]
KRONOLOGI	Tanggal unggahan membuktikan peredaran pada Oktober. Tanggal tidak membuktikan asal waktu materi yang diduga atau saat akses diperoleh.
HAL YANG DIBUKTIKAN	Iklan memuat jumlah tersebut, ketentuan komersial, dan klaim teks terminal. Jumlah mengacu pada populasi berbeda yang diiklankan.

ALTERNATIF	Penawaran dapat menggabungkan catatan lama dengan pernyataan akses. Narasi teknis atau tampilan terminal yang masuk akal tidak memastikan keaslian layanan atau hasil yang diduga.
BATAS	Keaslian, catatan unik, identitas berkas, kebaruan akses, dan hak yang diklaim belum dipastikan. Ketiga jumlah yang diiklankan tidak boleh dijumlahkan atau disebut orang unik.
RESPONS	Penanggung jawab aplikasi perlu meninjau perubahan berhak istimewa, integrasi, dan ekspor massal. Penanggung jawab identitas perlu memvalidasi akun relevan saat ini. Pemimpin penanganan insiden perlu menyimpan kesimpulan terpisah mengenai data dan akses.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B02 31 Okt 2026

marlanwg Iklan yang disimpan Forum Inggris

TEKS ASLI

[count redacted] distinct [redacted document type] submission records

TERJEMAHAN

[jumlah disamarkan] catatan pengajuan berbeda untuk [jenis dokumen disamarkan]

Catatan. Populasi yang diiklankan berbeda dan tidak boleh dijumlahkan; rujukan jenis dokumen disamarkan.

Hal yang dibuktikan
Iklan memuat klaim jumlah pengajuan, pengenal, dan kasus pengembalian dana beserta ketentuan komersial.

Belum dipastikan
Keaslian, keunikan catatan, identitas berkas, kebaruan akses, dan hak yang diklaim belum dipastikan.

KASUS C

C

Akses jarak jauh sektor pertanian membawa klaim hak akses

Klaim belum terverifikasi

Kartu bukti B03 29 Okt 2026 Iklan yang disimpan Organisasi pertanian

KLAIM	Pencantuman 29 Oktober mengiklankan akses OpenVPN yang melibatkan organisasi pertanian. Pencantuman mengklaim hak administrator server, sekitar 10,000 host, dan harga penawaran $1,000. [S1]
KRONOLOGI	Tanggal mencatat pencantuman. Tanggal tidak membuktikan awal atau durasi akses.

HAL YANG DIBUKTIKAN	Unggahan memberikan jenis akses, deskripsi hak, perkiraan ukuran jaringan, dan ketentuan komersial. Semua itu merupakan pernyataan penjual.
ALTERNATIF	Penawaran dapat diperantarai, tidak akurat, atau kedaluwarsa. Pencantuman pertanian lain tidak harus menyangkut organisasi atau akses yang sama.
BATAS	Identitas sasaran, keabsahan sesi, hak, inventaris host, dan transaksi belum dipastikan. Jumlah host yang diiklankan bukan jumlah perangkat terdampak yang diukur.
RESPONS	Penanggung jawab akses jarak jauh dan identitas perlu meninjau aktivitas masuk, keadaan akun, dan izin berhak istimewa yang relevan. Sesi tanpa izin yang terkonfirmasi memerlukan pembatasan dan penyelidikan sesuai cakupan.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B03 29 Okt 2026

CocoMel0n Iklan yang disimpan Forum Inggris

TEKS ASLI

Privilege ..... Server Admin

TERJEMAHAN

Hak akses ..... Administrator Server

Catatan. Jumlah host yang diiklankan bukan populasi perangkat terdampak yang diukur.

Hal yang dibuktikan
Pencantuman menyatakan jenis akses, hak yang diklaim, perkiraan ukuran jaringan, dan harga penawaran.

Belum dipastikan
Identitas sasaran, sesi aktif, hak akses, inventaris host, dan transaksi belum dipastikan.

D

KASUS D

Akses perguruan tinggi pada hari batas pengamatan memerlukan pemeriksaan keadaan saat ini

Klaim belum terverifikasi

Kartu bukti B04 22 Nov 2026 Iklan yang disimpan Perguruan tinggi

KLAIM	Unggahan 22 November mengiklankan akses VPN GlobalProtect ke suatu perguruan tinggi. Unggahan mengklaim hak administrator domain dan sekitar 10,000 host. Harga yang dinyatakan adalah 984,312 satoshi. [S1]

KRONOLOGI	Unggahan diamati pada hari batas pengamatan sebelum hari berakhir. Pengamatan tidak mewakili setiap publikasi berikutnya pada 22 November.
HAL YANG DIBUKTIKAN	Unggahan yang disimpan mengiklankan akses jarak jauh dan klaim peran berhak istimewa. Harga tetap dalam satuan aslinya.
ALTERNATIF	Penjual dapat mengedarkan penawaran kedaluwarsa atau belum terverifikasi. Catatan tidak menghubungkan penawaran perguruan tinggi ini dengan pencantuman pertanian Oktober.
BATAS	Identitas lembaga, sesi aktif, kemampuan administrator domain, jumlah host, dan penjualan belum dipastikan. Nilai fiat tidak disimpulkan.
RESPONS	Penanggung jawab identitas perlu meninjau aktivitas masuk VPN yang relevan, akun tidak aktif, dan perubahan kelompok berhak istimewa. Pencabutan sesi perlu mengikuti bukti internal saat ini dan keputusan respons sesuai cakupan.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B04 22 Nov 2026

AFKForever Iklan yang disimpan Forum Inggris

TEKS ASLI

Privilege ..... Domain Admin

TERJEMAHAN

Hak akses ..... Administrator Domain

Catatan. Harga tetap 984,312 satoshi; konversi fiat tidak disimpulkan. Pengamatan mendahului akhir hari batas pengamatan.

Hal yang dibuktikan

Unggahan pada hari batas pengamatan mengiklankan akses jarak jauh perguruan tinggi dan klaim izin berhak istimewa.

Belum dipastikan

Identitas lembaga, akses VPN aktif, kemampuan administrator domain, jumlah host, dan penjualan belum dipastikan.

KASUS E

E

Penawaran data identitas menyembunyikan platform yang diduga

Kartu bukti B05 | 21 Nov 2026 | Iklan yang disimpan

Platform verifikasi identitas yang tidak disebutkan namanya

Klaim belum terverifikasi

KLAIM	Unggahan 21 November mengiklankan lebih dari satu juta entri verifikasi identitas. Unggahan menjelaskan atribut identitas, data kontak atau perbankan, dan foto swafoto. Platform yang diduga tidak disebutkan namanya. [S1]
KRONOLOGI	Publikasi berada dalam periode terkini. Klaim penerimaan data harian yang terus berlangsung tidak membuktikan proses pengumpulan berkelanjutan yang diamati.
HAL YANG DIBUKTIKAN	Unggahan mencantumkan kategori informasi dan mengiklankan volume. Hal itu mendukung adanya penawaran materi identitas.
ALTERNATIF	Materi lama, penggabungan, atau deskripsi skema yang menyesatkan dapat menjelaskan penawaran. Daftar jenis data tidak mengidentifikasi pengendali.
BATAS	Sumber, keaslian, volume, keunikan, penerimaan data berkelanjutan, dan akses saat ini belum dipastikan. Jumlah bukan angka orang terdampak yang terkonfirmasi.
RESPONS	Penanggung jawab pencegahan penipuan perlu menguji pemeriksaan penggunaan ulang identitas. Penanggung jawab privasi dan insiden perlu menyimpan hubungan kredibel dengan data yang dikelola sebelum mengatribusikan penawaran kepada suatu platform.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B05 — 21 Nov 2026

SUB-ZERO | Iklan yang disimpan | Forum | Inggris

TEKS ASLI

Personal Data (PII) and Selfie Image

TERJEMAHAN

Data Pribadi (PII) dan Foto Swafoto

Catatan. Platform yang diduga tidak disebutkan namanya; deskripsi jenis data tidak mengidentifikasi pengendalinya.

Hal yang dibuktikan
Unggahan mengiklankan entri verifikasi identitas, kategori data, dan foto swafoto.

Belum dipastikan
Sumber, keaslian, volume, keunikan, penerimaan data berkelanjutan, dan akses saat ini belum dipastikan.

KASUS F

F

Pembeli dokumen mencari hubungan usaha nyata

Kartu bukti B06 | 4 Mar 2026 | Iklan yang disimpan | Dokumen identitas dan pendaftaran usaha

Klaim belum terverifikasi

KLAIM	Permintaan 4 Maret mencari dokumen identitas dan pendaftaran usaha Indonesia yang asli untuk perusahaan aktif. Permintaan menawarkan $100 per set dan ketentuan perantara. [S1]
KRONOLOGI	Tanggal mencatat permintaan pembelian. Tanggal tidak membuktikan pasokan atau penggunaan berikutnya.
HAL YANG DIBUKTIKAN	Pembeli secara tegas meminta dokumen yang belum kedaluwarsa dan menolak materi yang diedit atau palsu. Ini merupakan bukti sisi permintaan.
ALTERNATIF	Tujuan yang dimaksud tidak dinyatakan. Permintaan saja tidak dapat menentukan keabsahan hukum atau hasil aktivitas berikutnya.
BATAS	Pasokan, perpindahan dokumen, verifikasi berhasil, kewenangan perusahaan, dan transaksi belum dipastikan. Dokumen asli sendiri tidak membuktikan izin mewakili subjeknya.
RESPONS	Penanggung jawab penerimaan pelanggan perlu memverifikasi kewenangan pemohon melalui hubungan independen yang telah ditetapkan. Pemeriksaan dokumen perlu dihubungkan dengan usaha dan orang saat ini, dengan keputusan tercatat.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B06 4 Mar 2026

DrBisoun0urs | Iklan yang disimpan | Forum | Inggris

TEKS ASLI

WTB real KTP + NIB from Indonesia.

TERJEMAHAN

Ingin membeli KTP + NIB asli dari Indonesia.

Catatan. Istilah dokumen asli Indonesia dipertahankan; hasil permintaan belum dipastikan.

Hal yang dibuktikan

Pembeli meminta dokumen identitas dan usaha asli yang belum kedaluwarsa serta menolak materi yang diedit.

Belum dipastikan

Pasokan, perpindahan dokumen, verifikasi berhasil, kewenangan perusahaan, dan transaksi belum dipastikan.

KASUS G

G Iklan akun pesan berulang sepanjang waktu

Kartu bukti B07 | 5 Jan 2026 | Iklan yang disimpan | Akun pesan bernomor Indonesia

Klaim belum terverifikasi

KLAIM	Rangkaian berulang menawarkan akun pesan bernomor Indonesia dan format materi akun yang dapat digunakan kembali. Satu alias mengiklankan $0.45 pada Januari dan $0.40 menjelang akhir Februari atau Maret. [S1]
KRONOLOGI	Berkas kasus mencakup Januari hingga 21 November, dengan daftar penawaran tambahan pada 8 dan 19 November. Pengulangan membuktikan peredaran pada tanggal tersebut, bukan akses tanpa izin yang berlanjut.
HAL YANG DIBUKTIKAN	Daftar penawaran berulang dan iklan berikutnya secara tegas menyebut akun baru atau lama serta materi akun yang dapat digunakan kembali. Hal itu membuktikan klaim pasokan, bukan asal dari pencurian.
ALTERNATIF	Akun dapat baru didaftarkan, bukan dicuri. Alias dan daftar harga berbeda tidak membuktikan operator yang sama, berkas yang sama, atau tren harga seluruh pasar.
BATAS	Asal akun, identitas berkas, pembelian selesai, dan operasi bersama belum dipastikan. Iklan berulang bukan pelanggaran keamanan tambahan atau korban unik.

RESPONS	Penanggung jawab keamanan akun dan penipuan perlu meninjau pendaftaran, otomatisasi, dan perilaku sesi yang relevan. Penggunaan tanpa izin saat ini perlu ditangani melalui respons identitas sesuai cakupan.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B07 5 Jan 2026

sellingood | Iklan yang disimpan | Forum | Inggris

TEKS ASLI

Telegram Accounts for Sale - Desktop Tdata \ Session+Json Files

TERJEMAHAN

Akun Telegram Dijual - Desktop Tdata \ Berkas Session+Json

Catatan. Iklan pertama dalam rangkaian ini bertanggal 5 Januari; tanggal berikutnya tercantum dalam dosir.

Hal yang dibuktikan
Unggahan berulang mendukung rangkaian iklan; iklan Juli yang terpisah juga menjelaskan materi akun yang dapat dipindahtangankan.

Belum dipastikan
Asal akun, identitas berkas, pembelian selesai, dan operasi bersama belum dipastikan.

KASUS H

H Catatan alur kerja asuransi diiklankan berulang

Kartu bukti B08 | 12 Jan 2026 | Iklan yang disimpan | Platform alur kerja asuransi

Klaim belum terverifikasi

KLAIM	Unggahan menjelaskan sekitar 199,000 catatan alur kerja asuransi, termasuk pengajuan, riwayat API, materi terkait polis, dan data identitas. Kategori catatan bercampur. [S1]
KRONOLOGI	Judul terkait muncul pada 12 Januari, 18 Februari, dan 1 Oktober. Publikasi Oktober tidak membuktikan penyusupan baru pada Oktober.
HAL YANG DIBUKTIKAN	Judul mengulang penawaran. Narasi Oktober menjelaskan beberapa tabel dan kategori informasi.
ALTERNATIF	Materi lama yang dimiliki, klaim yang disalin, atau materi yang beredar kembali dapat menjelaskan deskripsi berulang. Judul dan jenis data serupa tidak membuktikan berkas identik.

BATAS	Kesamaan kumpulan data, asal, orang unik, akses saat ini, dan pelanggaran keamanan pada 2026 belum dipastikan. Jumlah baris bukan jumlah peserta asuransi.
RESPONS	Penanggung jawab data dan aplikasi perlu meninjau izin ekspor, otorisasi dokumen, dan log API sensitif. Kecocokan kredibel perlu masuk ke penilaian privasi dengan periode dan cakupan jenis data yang terbatas.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B08 — 12 Jan 2026

Darmanboy24 · Iklan yang disimpan · Forum · Inggris

TEKS ASLI

This dump includes policy applications, API history, loan data, ID cards (KTP)

TERJEMAHAN

Kumpulan data ini mencakup permohonan polis, riwayat API, data pinjaman, kartu identitas (KTP)

Catatan. Judul terkait muncul pada 12 Januari, 18 Februari, dan 1 Oktober; publikasi tidak membuktikan penyusupan baru.

Hal yang dibuktikan
Judul Januari, Februari, dan Oktober mengulang penawaran data alur kerja asuransi.

Belum dipastikan
Kesamaan kumpulan data, asal, orang unik, akses saat ini, dan pelanggaran keamanan pada 2026 belum dipastikan.

KASUS I

Kejadian layanan teknologi disajikan sebagai klaim data berjumlah besar

Klaim belum terverifikasi

Kartu bukti B09 · 12 Nov 2026 · Iklan yang disimpan · Perusahaan jasa teknologi

KLAIM	Unggahan 12 November mengenai perusahaan jasa teknologi mengiklankan sekitar 6.58 juta kejadian internal. Unggahan menjelaskan kategori data akun, pengguna, pengiriman kejadian, dan kredensial. [S1]
KRONOLOGI	Unggahan mengklaim kejadian lebih awal pada Oktober. Peredaran November tidak secara mandiri membuktikan tanggal aktivitas yang dinyatakan atau penyusupan baru pada November.
HAL YANG DIBUKTIKAN	Publikasi memuat klaim volume kejadian dan deskripsi data campuran. Publikasi menyatakan tidak ada tebusan yang terlibat.
ALTERNATIF	

Aliran kejadian yang disalin atau salah atribusi dapat menjelaskan materi. Skema dan narasi tidak memastikan keaslian penyedia atau berkas.

BATAS	Atribusi, identitas berkas, keabsahan rahasia, akses saat ini, dan jumlah pengguna unik belum dipastikan. Sebanyak 6.58 juta kejadian tidak boleh diubah menjadi 6.58 juta pengguna.
RESPONS	Penanggung jawab aplikasi dan identitas perlu meninjau ekspor dan hubungan kredensial yang relevan. Paparan tervalidasi perlu memicu rotasi kredensial sesuai cakupan dan peninjauan akses lanjutan.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B09 12 Nov 2026

updap | Iklan yang disimpan | Forum | Inggris

TEKS ASLI

6.58M Events [...]

TERJEMAHAN

6.58M Kejadian [...]

Catatan. Kejadian bukan pengguna; tanggal aktivitas Oktober yang diduga tetap merupakan klaim.

Hal yang dibuktikan

Unggahan mengiklankan aliran kejadian dengan campuran kategori data dan menyatakan tidak ada tebusan yang terlibat.

Belum dipastikan

Atribusi, identitas berkas, keabsahan rahasia, akses saat ini, dan jumlah pengguna unik belum dipastikan.

4.4 Enam berkas kasus eksternal

Kasus berikut menggunakan sumber publik yang telah dibaca. Kasus menggambarkan dampak dan batas bukti. Pemilihannya tidak membuktikan prevalensi relatif antar sektor. Hanya pengungkapan pengendali dalam Kasus J yang menyebut nama. Berkas lainnya menggunakan peran yang luas.

J

KASUS J

Fore Coffee mengungkap akses tanpa izin

Layanan konsumen

Pengungkapan pengendali

KLAIM

Fore Coffee mengonfirmasi akses tanpa izin ke platform pelanggannya. Cakupan awalnya hingga sekitar 5.7 juta akun. Ini merupakan pengungkapan pengendali, bukan dugaan yang hanya berasal dari penjual. [S44]

KRONOLOGI	Pemberitahuan diterbitkan pada 28 Oktober. Pada 5 November, pemberitaan mengutip Komdigi yang menyatakan laporan perusahaan diterima pada 28 Oktober. Pemeriksaan berikutnya merupakan bagian kasus yang sama. [S44][S45]
HAL YANG DIBUKTIKAN	Pengendali menjelaskan informasi kontak dan profil, PIN yang di-hash, serta riwayat pembelian yang berpotensi terdampak. Cakupan berbeda per pengguna. Pengendali menyatakan platform diamankan dalam 24 jam sejak deteksi. [S44]
ALTERNATIF	Jumlah akun awal dapat berubah selama penyelidikan. Satuan akun dalam pemberitahuan tidak membuktikan jumlah individu unik atau bahwa setiap jenis data terdampak pada setiap akun.
BATAS	Pengendali menyatakan nomor induk kependudukan (NIK), foto kartu tanda penduduk (KTP), dan informasi pembayaran tidak terdampak, tanpa indikasi penyalahgunaan saat pengungkapan. Temuan tersebut tetap diatribusikan kepada pengendali. Awal penyusupan dan tanggung jawab regulasi akhir belum dipastikan. [S44][S45]
RESPONS	Penanggung jawab aplikasi dan identitas perlu memvalidasi keadaan akun terdampak serta log akses yang tersedia. Penanggung jawab privasi perlu mencatat cakupan sesuai jenis data dan keputusan notifikasi. Operasional pelanggan perlu mendasarkan saran pada catatan kasus saat ini.

Kesimpulan

Akses tanpa izin diungkapkan; cakupan akun dan data masih sementara.

Pelajaran pertahanannya menyangkut ketepatan. Organisasi perlu membedakan informasi yang terkonfirmasi terdampak, berpotensi terdampak, dan berada di luar cakupan yang dinyatakan. Pembedaan yang sama perlu muncul dalam saran pelanggan, laporan regulator, dan pembaruan berikutnya.

Perubahan kata sandi atau PIN dapat menjadi salah satu langkah pelindungan. Perubahan tidak membuktikan sesi, jalur pemulihan, atau integrasi terkait telah ditinjau. Penyelesaian memerlukan bukti dari penanggung jawab identitas dan aplikasi yang relevan.

KASUS K

K

Penyelidikan bank daerah mengikuti kerugian transaksi

Jasa keuangan

Keterangan penyelidikan polisi

KLAIM	Polisi melaporkan penyusupan sistem bank daerah bertanggal 22 Februari 2026. Keterangan Juli melaporkan transfer dari rekening milik 6,609 nasabah dan sekitar Rp144 miliar kerugian. Angka tersebut merupakan angka yang dilaporkan penyelidikan polisi. [S36]
KRONOLOGI	Kuasa hukum bank melaporkan dugaan peretasan pada 23 Februari. Pemberitaan awal menjelaskan audit forensik dan pembatasan akses digital. Pengumuman polisi 15 Juli merupakan tindak lanjut kejadian Februari. [S36][S37]
HAL YANG DIBUKTIKAN	Keterangan awal mendukung adanya pengaduan dan pembatasan layanan. Keterangan polisi berikutnya menjelaskan konversi dana menjadi aset kripto dan sekitar Rp18.94 miliar aset yang dibekukan. Aset dibekukan berbeda dari uang yang dikembalikan kepada pelanggan. [S36][S37]
ALTERNATIF	Keterangan publik menjelaskan tahapan penyelidikan berbeda. Perkiraan awal, angka kerugian penyelidikan, dan kerugian akhir yang diputuskan merupakan hal terpisah.
BATAS	Dugaan terhadap tersangka bukan putusan pidana bersalah. Jumlah nasabah yang dilaporkan bukan jumlah korban ransomware. Sumber tidak mendukung pengaitan kejadian ini dengan label pemerasan yang terlihat di tempat lain.
RESPONS	Penanggung jawab kejahatan keuangan dan keamanan perlu merekonsiliasi bukti transaksi, catatan autentikasi, dan keluhan pelanggan. Pemimpin penanganan insiden perlu menyimpan tanggal aktivitas Februari beserta tonggak penyelidikan berikutnya. Tim hukum perlu melacak status dugaan.

Kesimpulan

Angka transaksi dan aset mempertahankan status penyelidikan dan satuannya.

Kasus ini menjadikan keutuhan transaksi sebagai perhatian utama insiden. Penyelidikan tidak perlu menunggu enkripsi atau unggahan pemerasan publik sebelum meninjau transfer tidak lazim dan perubahan akun.

Pelaporan pemulihan juga perlu mempertahankan satuan. Jumlah yang dibekukan, dugaan kerugian, dan jumlah penggantian menggambarkan hasil berbeda. Pimpinan perlu meminta bukti di balik setiap angka sebelum menerbitkan klaim pemulihan.

KASUS L

L

Penyelidikan sistem pendanaan melintasi dua tahun

Keuangan pendidikan

Keterangan penyelidikan polisi

KLAIM	Polisi menjelaskan akses brute-force ke sistem pendanaan pendidikan dan dua dugaan pencurian. Satu terjadi pada 17 Desember 2025. Kejadian lain pada 20 Januari 2026. [S35]
KRONOLOGI	Pengumuman diterbitkan pada 3 April 2026. Pengumuman mengaitkan Rp344,802,770 dengan kejadian Desember dan Rp598 juta dengan kejadian Januari. Hanya yang terakhir termasuk periode aktivitas laporan ini. [S35]
HAL YANG DIBUKTIKAN	Sumber mendukung keterangan penyelidikan resmi mengenai akses sistem dan kerugian keuangan. Sumber melaporkan akumulasi Rp942,802,770 pada kedua tanggal. Jumlah kumulatif itu tidak boleh disajikan seluruhnya sebagai kerugian 2026. [S35]
ALTERNATIF	Keterangan publik tidak membuktikan setiap pengguna sistem pendanaan memiliki kelemahan kontrol yang sama. Satu teknik yang dijelaskan juga tidak membuktikan kampanye nasional terhadap sektor.
BATAS	Ini merupakan penyelidikan polisi, bukan temuan pengadilan. Laporan tidak mengidentifikasi sekolah terdampak tambahan, menyimpulkan pengambilan data yang lebih luas, atau menghubungkan kasus dengan iklan akses yang tidak terkait.
RESPONS	Penanggung jawab keuangan dan identitas perlu meninjau pelindungan akun, persetujuan pembayaran, dan rekonsiliasi transaksi bersama. Catatan insiden perlu memisahkan tanggal dan jumlah setiap transaksi. Penanganan perlu mengatasi jalur akses yang tervalidasi.

Kesimpulan

Hanya transaksi Januari 2026 yang termasuk periode aktivitas ini.

Kasus ini menunjukkan perlunya kolom tanggal aktivitas dalam kronologi berdasarkan publikasi. Pengumuman 2026 dapat memuat kerugian tahun sebelumnya. Laporan tahunan perlu mempertahankan batas tersebut.

Kasus juga menunjukkan pelindungan akses dan persetujuan pembayaran saling melengkapi. Organisasi perlu menguji apakah aktivitas masuk tanpa izin dapat langsung berlanjut ke perubahan keuangan. Latihan perlu menghasilkan pengecualian dengan penanggung jawab dan perbaikan terverifikasi.

KASUS M

M

Pasar akses situs melayani penyalahgunaan konten

Situs lintas sektor

Keterangan penyelidikan polisi

KLAIM	Polisi menjelaskan penyelidikan yang melibatkan akses ke 260 situs. Rincian sektor mencakup 80 situs sekolah, 20 situs perguruan tinggi, 13 situs pemerintah, dan 147 situs perusahaan. [S38]
KRONOLOGI	Keterangan diterbitkan pada 30 Juli dan kemudian diperbarui pada 28 September. Pembaruan tidak membuktikan kelompok kedua berisi 260 penyusupan. Tanggal penyusupan setiap situs tidak diberikan. [S38]
HAL YANG DIBUKTIKAN	Polisi menyatakan akses dijual melalui sarana pesan untuk promosi perjudian. Panduan respons historis BSSN bertanggal Juni 2023 membahas situs pemerintah dan pendidikan yang menampilkan konten perjudian. Panduan tidak secara independen mengonfirmasi setiap situs yang diselidiki. [S38][S39]
ALTERNATIF	Model usaha yang diamati menyangkut akses situs dan penempatan konten. Model itu tidak membuktikan setiap situs mengalami pengambilan data atau satu jalur akses awal berlaku seluruhnya.
BATAS	Situs, lembaga, dan terdakwa merupakan satuan berbeda. Sebanyak 260 situs yang dilaporkan tidak boleh menjadi 260 korban terkonfirmasi dalam setiap kumpulan data lain. Iklan yang tampil sendiri tidak membuktikan akses ke sistem keuangan atau kepegawaian.
RESPONS	Penanggung jawab layanan web perlu meninjau akun berhak istimewa, perubahan penerapan, dan keutuhan konten. Tim insiden perlu menyimpan bukti sebelum pemulihan. Penutupan perlu mencakup jalur akses tervalidasi dan pemeriksaan akses menetap.

Kesimpulan

Akses situs dan penyalahgunaan konten tidak membuktikan pencurian data pada setiap situs.

Halaman utama yang bersih merupakan uji pemulihan yang belum lengkap. Perubahan konten dapat terlihat sementara akses tambahan tetap tersembunyi. Pemulihan perlu mencakup akses administrator, komponen aplikasi, dan jalur yang digunakan untuk menerbitkan konten.

Tanggung jawab sektoral juga penting. Tim teknologi pusat dapat mendukung banyak situs sementara unit kerja mengendalikan kredensial konten. Catatan pemulihan perlu mengidentifikasi tanggung jawab teknis dan administrasi konten.

KASUS N

N

Laporan aplikasi kepegawaian memuat perselisihan

Administrasi publik

Keterangan yang diperselisihkan

KLAIM	Pemberitaan mengutip dokumen BSSN yang menjelaskan 13 baris sampel kepegawaian dan dugaan akses terkait akun yang diperoleh melalui infostealer. [S40]
KRONOLOGI	Laporan menjelaskan penemuan pada 22 Juni, notifikasi daerah pada 23 Juni, dan dokumen BSSN bertanggal 24 Juni. Artikel diterbitkan pada 27 Juni. Tanggal tersebut mengacu pada tonggak kasus berbeda. [S40]
HAL YANG DIBUKTIKAN	Pejabat daerah mengakui notifikasi dan mitigasi. Pemberitaan menjelaskan kecocokan nama dan nomor telepon dalam sampel. Pejabat juga menyangkal kebocoran nyata atau dampak merugikan. Kedua posisi tetap ditampilkan. [S40]
ALTERNATIF	Kecocokan informasi sampel dapat mendukung keaslian sebagian baris tanpa membuktikan cara perolehannya. Kecocokan tidak secara independen membuktikan sesi berhak istimewa saat ini, pengambilan seluruh aplikasi, atau basis data baru yang berbeda.
BATAS	Pemberitaan menjelaskan dokumen BSSN dan tanggapan pejabat daerah. Perselisihan belum terselesaikan. Tiga belas baris sampel tidak membuktikan keseluruhan populasi terdampak.
RESPONS	Penanggung jawab identitas perlu memvalidasi akun yang terkait dan riwayat sesi. Penanggung jawab aplikasi perlu membandingkan izin akses dengan materi yang diduga. Penanggung jawab privasi dan insiden perlu mencatat hal yang belum dipastikan serta tindakan pelindungan.

Kesimpulan

Indikator paparan dan penyangkalan resmi tetap merupakan hal yang berbeda.

Penyangkalan dampak dan indikator paparan yang kredibel dapat muncul bersamaan saat bukti dinilai. Respons yang tepat adalah menguji pernyataan mengenai akun dan data. Keduanya tidak boleh dipastikan hanya berdasarkan judul.

Ini juga merupakan model bagi klaim penjual yang diperselisihkan. Penyelidikan dapat mencatat kecocokan sampel yang didukung bukti sambil menahan kesimpulan kompromi lebih luas. Hal ini memberikan dasar yang dapat dipertanggungjawabkan untuk pelindungan yang sebanding.

KASUS O

Situs layanan daerah menampilkan konten tanpa izin

Layanan publik daerah

Pejabat dikutip dalam pemberitaan

KLAIM	Pejabat e-government daerah mengonfirmasi dua situs telah menampilkan konten iklan tanpa izin. Pemberitaan menjelaskan iklan perjudian dan iklan komersial lainnya. Peran layanan tetap dibuat luas di sini. [S41]
KRONOLOGI	Pejabat menjelaskan penonaktifan situs pada 9 Agustus. Pemberitaan menyusul pada 10 Agustus. Tanggal itu mendukung tonggak respons dan publikasi, bukan awal penyusupan yang pasti. [S41]
HAL YANG DIBUKTIKAN	Keterangan mendukung penyalahgunaan konten yang terlihat dan keputusan menghapus akses publik selama respons. Keterangan juga menjelaskan administrasi konten yang tersebar. Keterangan tidak membuktikan seluruh layanan terkait memiliki akses yang sama. [S41]
ALTERNATIF	Pejabat mengemukakan kemungkinan paparan kredensial sebagai penjelasan. Keterangan publik tidak membuktikan penyebab utama itu. Kelemahan aplikasi atau jalur akses lain tidak dapat dipastikan dari pernyataan yang tersedia.
BATAS	Laporan tidak menyimpulkan pencurian data pribadi, manipulasi transaksi, atau kompromi jaringan pemerintah daerah yang lebih luas. Dua situs tidak menjadi tren insiden nasional.
RESPONS	Penanggung jawab layanan perlu menyimpan bukti konten dan akses, lalu memulihkan dari keadaan tepercaya. Penanggung jawab identitas perlu meninjau akun administrator. Penyelesaian perlu mencakup jalur publikasi yang diuji dan penanggung jawab konten yang ditetapkan.

Kesimpulan

Penyalahgunaan konten yang terlihat didukung bukti; jalur akses awal belum dipastikan.

4.5 Penawaran akses dan pemerasan tambahan

P

KASUS P

Penawaran asuransi kesehatan mengklaim akses dan data

Kartu bukti B10 | 5 Mei 2026 | Iklan yang disimpan | Organisasi asuransi kesehatan

Klaim belum terverifikasi

KLAIM	Iklan 5 Mei mengklaim akses dan kumpulan catatan berskala sangat besar yang melibatkan organisasi asuransi kesehatan. Unggahan 7 Mei mengulang klaim, diikuti balasan 12 Mei. [S1]
KRONOLOGI	Tanggal menjelaskan peredaran. Tanggal tidak membuktikan penyusupan baru pada setiap tanggal atau periode yang diwakili catatan yang diduga.
HAL YANG DIBUKTIKAN	Iklan menghubungkan akses dengan data identitas, keanggotaan, klinik, rujukan, dan diagnostik. Balasan berikutnya mengutip penawaran yang sama.
ALTERNATIF	Materi lama, penggabungan, cakupan yang dibesarkan, atau deskripsi palsu dapat menjelaskan penawaran. Arsip lama tidak membuktikan akses saat ini.
BATAS	Keaslian, kebaruan akses, ekspor, populasi unik, dampak pelanggan, dan transaksi belum dipastikan. Jumlah yang diiklankan bukan cakupan nasional atau orang terkonfirmasi.
RESPONS	Penanggung jawab data dan layanan perlu meninjau kueri massal, ekspor, dan izin akun layanan yang relevan. Akses sensitif untuk diagnostik atau rujukan perlu memiliki penanggung jawab dan cakupan terdokumentasi.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B10 — 5 Mei 2026

alwayschina | Iklan yang disimpan | Forum | Inggris

TEKS ASLI

[ACCESS + DB] [a health-insurance organisation] – [record count redacted]

TERJEMAHAN

[AKSES + DB] [suatu organisasi asuransi kesehatan] – [jumlah catatan disamarkan]

Catatan. Jumlah catatan yang diiklankan disamarkan; jumlah itu bukan cakupan nasional atau orang terkonfirmasi.

Hal yang dibuktikan
Iklan Mei menggabungkan klaim akses dengan klaim data berjumlah besar; balasan berikutnya mengutip penawaran tersebut.

Belum dipastikan
Keaslian, akses saat ini, populasi unik, dampak pelanggan, ekspor, dan transaksi belum dipastikan.

KASUS Q

Unggahan sektor pertanian menuntut pembayaran untuk penghapusan

Klaim belum terverifikasi

Kartu bukti B11 | 14 Mei 2026 | Iklan yang disimpan | Badan publik bidang pertanian

KLAIM	Unggahan 14 Mei mengklaim lebih dari 243 GB informasi yang melibatkan badan publik bidang pertanian. Unggahan menuntut $10,000 untuk penghapusan sebelum publikasi. [S1]
KRONOLOGI	Unggahan menjelaskan pengumpulan yang berlanjut. Pernyataan itu tidak membuktikan penyusupan berkelanjutan yang diamati.
HAL YANG DIBUKTIKAN	Pesan memuat tuntutan pembayaran untuk penghapusan serta menjelaskan dokumen, informasi pegawai, dan data organisasi.
ALTERNATIF	Volume dapat dibesarkan atau pengumpulan yang diklaim dapat mencam-purkan materi publik, pribadi, dan lama. Tuntutan tidak secara independen membuktikan kendali atas materi yang diduga.
BATAS	Identitas arsip, ukuran, kompromi, kemampuan penghapusan, pembayaran, dan hasil publikasi belum dipastikan. Jumlah yang diminta bukan kerugian.
RESPONS	Pemimpin penanganan insiden perlu menyimpan ancaman dan memban-dingkannya dengan bukti akses serta ekspor internal. Penanggung jawab hukum, privasi, dan kesinambungan perlu menyiapkan keputusan mengenai sistem dan data yang benar-benar terlibat.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B11 14 Mei 2026

Kyyzo Iklan yang disimpan Forum Inggris

TEKS ASLI

We are demanding a ransom of $10,000 to delete all the data

TERJEMAHAN

Kami meminta tebusan $10,000 untuk menghapus seluruh data

Catatan. Permintaan bukan bukti pembayaran, penghapusan, atau kendali atas arsip yang telah ditunjukkan.

Hal yang dibuktikan
Unggahan meminta pembayaran untuk penghapusan serta menjelaskan informasi organisasi, dokumen, dan pegawai.

Belum dipastikan
Identitas arsip, ukuran, kompromi, kemampuan penghapusan, pembayaran, dan hasil publikasi belum dipastikan.

R

KASUS R

Daftar penawaran kotak surat resmi menyiratkan kewenangan yang tidak dibuktikannya

Klaim belum terverifikasi

Kartu bukti B12 | 12 Jun 2026 | Iklan yang disimpan | Identitas kotak surat otoritas publik

KLAIM	Daftar penawaran Januari dan unggahan Juni menawarkan dugaan akses kotak surat terkait penegakan hukum seharga $200. Teks Juni mempromosikan penyalahgunaan saluran permintaan resmi. [S1]
KRONOLOGI	Tanggal yang disimpan adalah 31 Januari dan 12 Juni. Tanggal tersebut membuktikan iklan, bukan sesi berkelanjutan di antara kedua tanggal.
HAL YANG DIBUKTIKAN	Daftar penawaran menyatakan negara, peran otoritas publik, dan harga. Pesan berikutnya membahas permintaan kepada platform daring.
ALTERNATIF	Akses dapat palsu, kedaluwarsa, terbatas, atau salah label. Bahkan kepemilikan kotak surat sendiri tidak membuktikan kewenangan hukum atau hak atas layanan platform.
BATAS	Kepemilikan kotak surat, akses saat ini, hak permintaan, tindakan yang disetujui penerima, dan transaksi belum dipastikan. Daftar penawaran bukan bukti penyamaran identitas yang berhasil.
RESPONS	Tim penerima permintaan data khusus perlu memverifikasinya melalui saluran independen yang telah ditetapkan. Penanggung jawab identitas perlu meninjau aktivitas masuk, penerusan, dan aturan kotak surat tidak lazim jika bukti mengidentifikasi akun relevan.

Kesimpulan

Publikasi diamati; akses, keaslian, dan hasil memerlukan validasi untuk setiap hal yang diklaim.

Kartu bukti B12 12 Jun 2026

Governer Iklan yang disimpan Forum Inggris

TEKS ASLI

Selling Government & Law Enforcement Email Accounts

TERJEMAHAN

Menjual Akun Email Pemerintah dan Penegakan Hukum

Catatan. Berkas kasus juga memuat daftar penawaran 31 Januari. Iklan Juni yang dikutip tidak membuktikan keberhasilan penyalahgunaan saluran permintaan.

Hal yang dibuktikan

Daftar penawaran mengiklankan kotak surat otoritas publik dan harga; unggahan berikutnya membahas permintaan data khusus.

Belum dipastikan

Kepemilikan kotak surat, akses saat ini, hak mengajukan permintaan, tindakan yang disetujui penerima, dan transaksi belum dipastikan.

4.6 Data berulang tidak membuktikan penyusupan berulang

Keterangan Komdigi pada 2 Oktober menyatakan BSSN menjelaskan informasi yang beredar belakangan sebagai data lama yang beredar kembali. Otoritas melanjutkan koordinasi mengenai penjualan data melawan hukum. Keterangan tersebut menyangkut materi yang dibahas dalam pemberitahuan. [S46]

Keterangan tidak boleh digeneralisasi ke setiap penawaran saat ini. Unggahan berbeda dapat menyangkut materi atau periode berbeda. Sebaliknya, publikasi pada Oktober sendiri tidak membuktikan penyusupan Oktober.

Karena itu, catatan kasus perlu mempertahankan empat pertanyaan terpisah. Kapan materi berasal? Kapan akses diduga? Kapan unggahan diterbitkan? Apa yang kemudian dibuktikan organisasi atau otoritas?

4.7 Periode terkini memiliki batas tersendiri

Ransompedia mencatat sembilan pencantuman pada November hingga batas pengamatan 22 November: tiga dari 1 hingga 7 November dan enam dalam periode terkini antara 8 dan 22 November. Pengamatan dihimpun sebelum 22 November berakhir. Angka tidak mencakup publikasi berikutnya pada hari itu atau setiap insiden siber dalam periode tersebut. [S2]

Periode yang sama memuat publikasi riset Check Point pada 10 November, pemberitahuan kesiapsiagaan pemerintah, dan imbauan layanan global BSSN. Semuanya merupakan kejadian publikasi dan koordinasi dengan tanggal dasar berbeda. [S28][S48][S50]

Pelaporan terkini perlu meningkatkan perhatian terhadap ketergantungan layanan yang relevan. Pelaporan tidak boleh menyatukan peringatan, pencantuman, dan gangguan layanan menjadi satu jumlah serangan. Bab 6 mempertahankan pembedaan tersebut dalam kronologi dan panel perbandingannya.

4.8 Tema tambahan mempertahankan batas yang lebih sempit

Tema	Tanggal peredaran	Hal yang didukung dan batasnya
Akun staf perguruan tinggi	2 Agustus dan 17 Oktober	Klaim berulang menyangkut akun staf dan materi terkait kata sandi; keabsahan saat ini dan identitas berkas belum dipastikan
Catatan pembayaran layanan publik	14 Januari hingga 11 Februari	Peredaran unggahan ulang belum terverifikasi; pengunggah menyatakan bukti tidak tersedia dan meragukan keakuratannya. Klaim transaksi tidak membuktikan orang atau akses infrastruktur
Catatan perbankan daerah	21 Januari dan 24 April	Judul yang menyebut masa lalu dan campuran kategori pelanggan, kartu, serta log tidak membuktikan pelanggaran keamanan baru pada 2026
Materi analitik sektor publik	7 Oktober	Klaim ekspor, berkas, model, dan baris tidak memastikan asal produksi atau akses saat ini
Informasi terkait bantuan dan disabilitas	Januari hingga Oktober	Kategori data sensitif perlu divalidasi; volume, asal, dan pernyataan politik belum dipastikan
Informasi ritel dan pemasok	Maret hingga November	Unggahan Maret dan April mengulang dugaan kejadian 10 Maret. Jumlah baris versi gratis dan lengkap bertumpang tindih; kejadian baru pada April dan identitas berkas belum dipastikan
Materi pendaftaran identitas daerah	8–19 November	Penawaran terkini mencakup catatan yang secara tegas disebut lebih lama; tanggal publikasi bukan tanggal pelanggaran keamanan
Materi keanggotaan koperasi	16 Oktober hingga 19 November	Penawaran berikutnya berisi 75,086 entri tidak membuktikan orang unik atau akses yang berlanjut
Materi identitas terkait pendidikan	14–22 November	Klaim siswa, alumni, guru, dan staf memuat jumlah baris atau lembar yang bertumpang tindih
Aplikasi keuangan sektor transportasi	17 Oktober	Dugaan kemampuan manipulasi buku besar tidak membuktikan eksploitasi, entitas pengguna layanan terdampak, atau perubahan pembayaran berhasil

Tema	Tanggal peredaran	Hal yang didukung dan batasnya
Pemberitahuan kredensial otomatis	Sejak 26 Juni	Label yang menyerupai sasaran tidak membuktikan pelanggaran keamanan organisasi atau kredensial yang berfungsi
Data personel otoritas publik	Februari hingga November	Unggahan ulang tidak membuktikan penyusupan baru. Unggahan April memberikan jumlah yang bertentangan, 417,000 dibandingkan 417, dan menjelaskan akses tahun sebelumnya
Data pesanan dan administrasi jasa kurir	18 April	Penjual mengklaim akses administrasi berkelanjutan dan pasokan data harian; keberlanjutan akses, identitas pelanggan, dan transaksi belum dipastikan
Daftar penawaran akses jarak jauh keuangan dan pertanian	13 Mei	Daftar penawaran VPN pada hari yang sama tidak membuktikan akses saat ini, kepemilikan sistem oleh pihak Indonesia, atau hubungan dengan penawaran lain
Permintaan data, tenaga verifikasi, dan pasokan SIM	Februari hingga November	Permintaan pembeli tidak membuktikan tujuan penggunaan, persetujuan, pasokan, verifikasi yang diterima, atau transaksi selesai
Pemerasan terhadap perusahaan dan penyedia layanan	2–17 Mei	Dugaan penjual mengenai hubungan penyedia, tuntutan belum dibayar, dan pengungkapan bertahap tidak membuktikan penyusupan bersama atau hasil pengungkapan
Penggabungan data dan asalnya	Januari hingga Oktober	Pernyataan pengunggah menjelaskan materi yang dikumpulkan dari forum; koleksi data untuk pencarian yang diiklankan tidak membuktikan penyusupan baru, asal, atau orang unik
Arsip klinis dan tenaga kesehatan	Februari hingga Mei	Klaim terkait kesehatan yang terpisah belum terverifikasi; populasi yang diiklankan tidak digabungkan dengan penawaran asuransi kesehatan
Akses organisasi sektor pangan	13 Februari	Klaim data internal dan akses berkelanjutan menyisakan identitas sistem, keaslian, akses saat ini, dan transaksi yang belum dipastikan

Tema yang disimpan ini memperluas cakupan keputusan tanpa menambah insiden terkonfirmasi. Jumlah catatan yang diiklankan tidak digabungkan. Tema ini tidak dihitung sebagai insiden terkonfirmasi. [S1]

4.9 Pengamatan tambahan mengenai layanan dan penyampaian ulang klaim

Suplemen terkait organisasi memiliki batas cakupan tersendiri dan tidak digabungkan ke basis korpus 19,814 unggahan yang disimpan. Peringatan yang disampaikan ulang juga tetap dibedakan dari catatan pencantuman Ransompedia. Klaim tambahan ini bukan jumlah insiden nasional. [S1][S2]

Tema	Tanggal publikasi	Hal yang didukung dan batasnya
Daftar penawaran akses situs dan hosting	Januari hingga November	Penjual mengiklankan akses administrasi atau hosting; balasan memperselisihkan tangkapan layar atau status akses. Kepemilikan, akses saat ini, dan transaksi belum dipastikan
Layanan publikasi dokumen hukum	7 Agustus	Iklan mengklaim sesi administrator aktif dan izin publikasi. Hak akses, keabsahan sesi, dan perubahan dokumen belum dipastikan
Daftar penawaran pembuatan akun keuangan	Januari hingga November	Penjual menjelaskan penyediaan materi identitas sementara pembeli menyediakan rincian kontak. Hal ini tidak membuktikan pencurian akun yang sudah ada, penyusupan bank, verifikasi yang diterima, atau transaksi
Catatan pendaftaran komunikasi	11 November	Penawaran data pendaftaran mengklaim tanggal internal 8 November; asal, identitas berkas, volume, dan akses saat ini belum dipastikan
Penyampaian ulang klaim pemerasan sektor energi	31 Juli	Pesan terusan mengatribusikan dugaan kepada Thegentlemen. Klaim dokumen teknik atau kendali industri tidak membuktikan akses atau gangguan sistem operasional
Penyampaian ulang klaim pemerasan bank daerah	17 November	Pesan terusan mengatribusikan klaim kepada Panzer. Pesan itu tidak membuktikan keaslian klaim primer, dampak, atau kesamaan dengan kejadian perbankan terdahulu
Templat penyalahgunaan pelaporan kepada dukungan	18 Oktober	Templat yang beredar mempromosikan penyalahgunaan pelaporan akun; pengiriman, pengaduan yang diterima, pembatasan akun, dan dugaan yang mendasarinya belum dipastikan

Penanggung jawab layanan perlu menghubungkan klaim ini dengan catatan akses yang disahkan dan keutuhan dokumen. Tim antipenipuan perlu mempertahankan pembedaan antara pembuatan akun yang diiklankan dan penyalahgunaan yang terbukti. Penyampaian ulang klaim tidak boleh mewarisi status pencantuman yang diamati secara terpisah.

TEMUAN UTAMA

01

Nyatakan hal yang didukung setiap klaim

02

Pisahkan tanggal aktivitas dan publikasi

03

Tutup penyelidikan dengan catatan validasi dan penanggung jawab

BAB 05

Keputusan per sektor

05

PERTANYAAN BAB INI

Bagaimana makna sinyal akses atau data yang sama berubah antar sektor?

8

Kelompok sektor gabungan dalam tampilan pencantuman terkait pemerasan

5.1 Distribusi sektor menggambarkan pencantuman 58
5.2 Layanan publik memerlukan tanggung jawab pada tingkat aplikasi 59
5.3 Pendidikan menggabungkan akses web dan alur kerja keuangan 59
5.4 Layanan konsumen memerlukan komunikasi sesuai jenis data 60
5.5 Pemasok digital dapat menimbulkan ketergantungan yang tidak seimbang 60
5.6 Dampak industri dan kesehatan memerlukan kehati-hatian 61
5.7 Catatan validasi bersama mendukung penanggung jawab yang berbeda 61

BAB 05

Keputusan per sektor

RINGKASAN

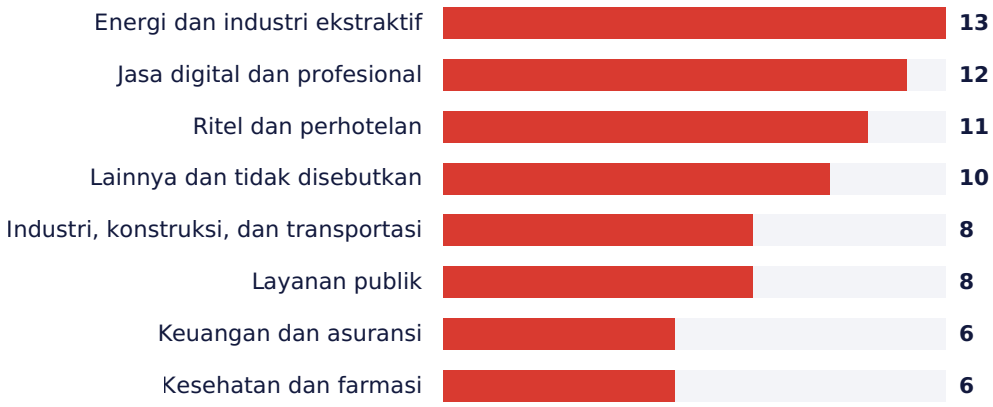
Dampak sektoral bergantung pada layanan dan izin yang terlibat. Sebanyak 74 pencantuman Ransompedia tersebar di delapan kelompok sektor gabungan. Kasus resmi menunjukkan dampak keuangan, aplikasi, dan situs. Jumlah pencantuman tidak mengukur gangguan atau kerugian layanan. Tim sektoral perlu menggunakannya untuk menguji prioritas paparan dan pemulihan terhadap operasinya sendiri. Tetapkan penanggung jawab layanan untuk setiap sinyal yang relevan, lalu minta bukti cakupan akses, dampak data, dan kemampuan pemulihan.

5.1 Distribusi sektor menggambarkan pencantuman

Energi dan industri ekstraktif mencakup 13 pencantuman Ransompedia. Jasa digital dan profesional mencakup 12, diikuti ritel dan perhotelan dengan 11. Ketiga kelompok ini mencakup 36 dari 74 pencantuman. [S2]

Pemusatan tersebut menggambarkan populasi pencantuman yang disimpan. Hal itu tidak menunjukkan sektor dengan dampak nasional terbesar. Organisasi yang tercantum dapat mengalami hasil berbeda, termasuk dugaan yang belum didukung bukti tambahan.

Pencantuman terkait pemerasan tersebar di delapan kelompok sektor



Sumber: pencantuman terkait pemerasan berlabel negara di Ransompedia, 1 Januari–22 November 2026; hari terakhir parsial [S2]. Klaim pencantuman bukan insiden terkonfirmasi, korban unik, atau penyusupan berhasil.

Kelompok sektor	Pencantuman	Keputusan yang didukung	Hal yang belum dibuktikan
Energi dan industri ekstraktif	13	Tinjau kesinambungan dan ketergantungan pemasok dengan akses berhak istimewa	Gangguan operasional atau dampak keselamatan
Jasa digital dan profesional	12	Periksa akses ke pelanggan serta tanggung jawab pemberitahuan pelanggan	Kompromi setiap pelanggan

Kelompok sektor	Pencantuman	Keputusan yang didukung	Hal yang belum dibuktikan
Ritel dan perhotelan	11	Validasi pelindungan platform pelanggan dan identitas	Penipuan atau kerugian konsumen nasional
Lainnya dan tidak disebutkan	10	Pastikan konteks layanan sebelum memprioritaskan kontrol	Satu kampanye bersama yang utuh
Industri, konstruksi, dan transportasi	8	Identifikasi ketergantungan penjadwalan, pengiriman, dan produksi	Kejadian operasional di seluruh sektor
Layanan publik	8	Pastikan keberlakuan IIV, penanggung jawab layanan, dan jalur pelaporan	Kompromi sistem pemerintah pusat
Keuangan dan asuransi	6	Hubungkan sinyal akses dengan kontrol transaksi dan pelaporan	Seluruh penipuan keuangan atau akun terdampak
Kesehatan dan farmasi	6	Uji ketersediaan dan respons data sensitif	Dampak pada pasien atau gangguan kesehatan yang terukur

5.2 Layanan publik memerlukan tanggung jawab pada tingkat aplikasi

Kasus aplikasi kepegawaian memuat indikator paparan, penerimaan notifikasi yang diakui, dan hasil yang diperselisihkan. Kasus situs layanan daerah mengonfirmasi penyalahgunaan konten yang terlihat. Penanggung jawab kontrol dan dampak datanya berbeda. [S40][S41]

Karena itu, program keamanan layanan publik perlu mengidentifikasi penanggung jawab setiap aplikasi dan jalur publikasi. Koordinasi pusat berguna, tetapi inventaris layanan pusat tetap dapat melewatkan kredensial unit kerja dan kewenangan administrasi konten yang didelegasikan.

Untuk setiap aplikasi, penanggung jawab layanan perlu mengetahui pengendali data, identitas berhak istimewa, akses pemasok, dan jalur pemulihan. Catatan insiden perlu menjelaskan unsur mana yang benar-benar terkait dengan bukti.

Penetapan sebagai IIV mengubah tanggung jawab pelaporan. Penetapan tersebut tidak berarti semua situs organisasi yang sama memiliki tingkat kekritisan yang identik. Penanggung jawab hukum dan layanan perlu memelihara pemetaan itu sebelum insiden.

5.3 Pendidikan menggabungkan akses web dan alur kerja keuangan

Laporan polisi menjelaskan penyalahgunaan situs terkait sekolah dan penyelidikan keuangan sistem pendanaan. Kasus pertama menyangkut penjualan akses situs. Kasus kedua menjelaskan dugaan aktivitas keuangan tanpa izin. [S35][S38]

Respons sektor perlu mempertahankan pembedaan tersebut. Rencana pemulihan situs tidak boleh menggantikan kontrol persetujuan pembayaran dan rekonsiliasi. Peninjauan keuangan tidak boleh menganggap situs publik sebagai jalur masuk.

Organisasi pendidikan perlu mengidentifikasi akun yang menghubungkan aplikasi administrasi dengan alur pembayaran. Organisasi juga perlu menguji cara staf sementara dan pemasok memperoleh, mempertahankan, serta kehilangan akses.

Bukti penyelesaian perlu sesuai dengan alur kerjanya. Peninjauan keutuhan konten menutup temuan situs. Rekonsiliasi transaksi dan peninjauan akses menutup temuan kontrol keuangan. Keduanya tidak saling menggantikan.

5.4 Layanan konsumen memerlukan komunikasi sesuai jenis data

Pengungkapan platform pelanggan membahas populasi akun sementara dan jenis data yang berbeda-beda. Keterangan pengendali tidak membuktikan bahwa setiap jenis data berlaku bagi setiap pengguna. Jumlah akun juga tidak sama dengan jumlah orang unik yang terdampak. [S44]

Operasional pelanggan perlu menyiapkan pesan yang mempertahankan batas tersebut. Saran perlu menjelaskan hal yang harus diperiksa pengguna dan cara dukungan resmi berkomunikasi. Respons perlu menghindari konfirmasi rincian yang belum dibuktikan penyelidikan.

Penanggung jawab aplikasi perlu meninjau hubungan antara informasi kontak, mekanisme pemulihan, dan riwayat transaksi. Kejadian data pelanggan dapat meningkatkan risiko penyamaran identitas meskipun pengendali mengecualikan informasi pembayaran dari kategori yang terdampak.

Hal itu merupakan implikasi perencanaan, bukan bukti penipuan berikutnya. Tim antipenipuan perlu memantau pola yang relevan dan mendokumentasikan pengamatan nyata. Laporan tidak mengubah dampak potensial menjadi hasil terukur.

5.5 Pemasok digital dapat menimbulkan ketergantungan yang tidak seimbang

Pencantuman layanan digital perlu diikuti peninjauan izin dan integrasi yang berhubungan dengan pelanggan. Pertanyaan pentingnya adalah layanan dan kredensial mana yang dapat dijangkau pemasok. Nama pemasok dalam unggahan pemerasan tidak menjawabnya.

Pelanggan perlu memiliki jalur yang disepakati untuk pertanyaan mendesak kepada pemasok. Jalur tersebut perlu meminta cakupan akses, status layanan, dan tindakan pelindungan. Hindari meminta pemasok memvalidasi atribusi pelaku yang tidak didukung bukti.

Layanan bersama juga dapat menimbulkan dampak ketersediaan tanpa penyusupan pada pemasok. Kejadian pemblokiran November menunjukkan pentingnya memasukkan ketergantungan pengembangan dan perangkat lunak dalam perencanaan kesinambungan. [S47]

Penanggung jawab layanan perlu menguji pilihan pengganti untuk ketergantungan eksternal yang kritis. Kontrak pemasok yang terdokumentasi membantu, tetapi latihan pengalihan yang diamati memberikan bukti berbeda.

5.6 Dampak industri dan kesehatan memerlukan kehati-hatian

Populasi pencantuman mencakup kelompok industri, transportasi, energi, dan kesehatan. Populasi itu tidak membuktikan gangguan produksi, logistik, perawatan klinis, atau keselamatan. Dampak tersebut memerlukan bukti tingkat layanan. [S2]

Perencanaan tetap perlu mempertimbangkan ketergantungan itu. Organisasi dapat mengidentifikasi layanan identitas, platform pengelolaan, dan pemasok yang mendukung kesinambungan operasional. Organisasi dapat menguji pemulihan tanpa menyatakan bahwa organisasi sejenis yang tercantum mengalami insiden operasional.

Organisasi kesehatan juga perlu membedakan data klinis, administrasi bisnis, dan situs publik. Klaim mengenai salah satunya tidak boleh digambarkan sebagai kompromi ketiganya.

5.7 Catatan validasi bersama mendukung penanggung jawab yang berbeda

Keputusan sektoral	Validasi pertama	Pemicu eskalasi	Bukti penyelesaian
Dugaan data sensitif	Bandingkan jenis data dan periode yang diduga dengan data yang dikelola	Kecocokan yang kredibel atau bukti akses saat ini	Penilaian cakupan data yang terbatas
Akses pemasok berhak istimewa	Pastikan akun, izin, dan hubungan layanan	Sesi tanpa izin yang aktif atau perubahan yang belum terjelaskan	Peninjauan akses dan keputusan penanganan pemasok
Manipulasi keuangan	Rekonsiliasi transaksi dan kejadian autentikasi	Perubahan tanpa izin atau transfer yang belum terjelaskan	Catatan kasus transaksi dan tindakan pelanggan
Penyalahgunaan situs	Tinjau konten, akses berhak istimewa, dan riwayat penerapan sistem	Perubahan tanpa izin atau indikator akses menetap	Pemulihan tepercaya dan perbaikan jalur akses
Peringatan ketersediaan	Bandingkan telemetri layanan dengan dampak yang diklaim	Penurunan layanan terukur yang sesuai dengan kronologi	Catatan dampak layanan dan pemulihan

Tugas-tugas tersebut perlu menggunakan pengenal kasus yang sama ketika berkaitan dengan kejadian yang sama. Tanggung jawab bersama atas fakta tidak mengharuskan satu tim melakukan seluruh penyelidikan.

Keputusan eksekutifnya adalah mendanai proses serah terima. Sinyal perlu mencapai fungsi yang dapat memvalidasinya. Penutupan perlu menyatakan hal yang telah dibuktikan, hal yang belum diketahui, dan tindakan tingkat layanan yang mengikuti.

TEMUAN UTAMA

01

Gunakan jumlah sektoral sebagai pengamatan pencantuman

02

Sesuaikan validasi dengan alur kerja terdampak

03

Minta bukti khusus layanan sebelum menjelaskan dampak operasional

BAB 06

Gangguan dan penilaian klaim

PERTANYAAN BAB INI

Bagaimana tim pertahanan bertindak atas peringatan sambil tetap memisahkan klaim serangan dan gangguan layanan?

6

Pencantuman terkait pemerasan terkini, bukan jumlah seluruh insiden terkini

6.1 Peringatan dapat mendasari persiapan 64
6.2 Kronologi dengan jenis bukti 64
6.3 Bandingkan hal yang dibuktikan, bukan jumlah yang bersaing 65
6.4 Bukti ketersediaan perlu mempertahankan dimensinya 66
6.5 Gangguan layanan membuka peluang penipuan 67
6.6 Komunikasikan hal yang didukung catatan layanan 67
6.7 Akses teknologi berhak istimewa memerlukan tujuan yang sah 67

BAB 06

Gangguan dan penilaian klaim

RINGKASAN

Periode terkini memuat pencantuman terkait pemerasan, pemberitahuan kesiapsiagaan, publikasi riset vendor, dan imbauan layanan global. Jenis bukti tersebut berbeda. Komdigi tidak memverifikasi keaslian atau kemampuan di balik ancaman dalam pemberitahuan kesiapsiagaannya. Imbauan gangguan layanan BSSN meneruskan penjelasan yang tidak menunjukkan aktivitas berbahaya. Tim pertahanan tetap perlu bersiap menghadapi gangguan, mencatat dampak terukur, dan mewaspadai penipuan oportunistis. Tetapkan satu penanggung jawab insiden untuk mencocokkan klaim dengan telemetri layanan sebelum mengeluarkan pernyataan dampak.

6.1 Peringatan dapat mendasari persiapan

Pemberitahuan Komdigi pada 10 November meneruskan imbauan BSSN pada 8 November dan surat berikutnya mengenai sistem publik. Pemberitahuan menjelaskan potensi gangguan serta menganjurkan pemantauan, pembaruan keamanan, autentikasi, dan kesiapan pemulihan. Kemampuan pelaku dan keaslian ancaman masih belum terverifikasi. [S48]

Hal ini mendukung keputusan kesiapan. Pemberitahuan itu tidak membuktikan bahwa DDoS, perubahan tampilan situs, manipulasi DNS, atau phishing telah berhasil terhadap setiap organisasi yang diperingatkan. Skenario dalam imbauan tetap merupakan skenario hingga didukung bukti kejadian.

Respons operasional perlu mempertahankan pembedaan tersebut. Pemimpin penanganan insiden dapat meningkatkan kesiapan, memeriksa kontak, dan meninjau layanan yang terpapar. Komunikasi perlu menjelaskan persiapan sebagai persiapan.

Peningkatan pemantauan juga memerlukan kondisi penghentian. Penanggung jawab perlu menyatakan sinyal layanan yang akan memicu eskalasi dan pengamatan yang mendukung kembalinya kesiapan rutin.

6.2 Kronologi dengan jenis bukti

30 Jul 2026	**Kepolisian** Melaporkan penyelidikan penjualan akses 260 situs; tanggal penyusupan setiap situs tidak diberikan [S38]
2 Okt 2026	**Komdigi** Menjelaskan peredaran kembali data lama yang dibahas dalam pemberitahuannya [S46]
17 Okt 2026	**updap** Mengiklankan dugaan akses backend perbankan dan sistem promosi [S1]

29 Okt 2026	**CocoMel0n** Mengiklankan akses jarak jauh sektor pertanian dengan klaim hak administrator [S1]
31 Okt 2026	**marlanwg** Mengiklankan data dan akses berhak istimewa yang melibatkan layanan pendapatan sektor publik [S1]
8 Nov 2026	**Komdigi** Melaporkan gangguan akses akibat pemblokiran yang terjadi pada 6 November [S47]
10 Nov 2026	**Komdigi** Meneruskan pemberitahuan kesiapsiagaan sistem publik sementara keaslian ancaman belum dipastikan [S48]
13 Nov 2026	**BSSN** Meneruskan penjelasan gangguan layanan global tanpa indikasi aktivitas berbahaya [S50]
18 Nov 2026	**Kepolisian** Menerbitkan keterangan pemberhentian karena pelanggaran etik dengan pengajuan banding; dugaan pidana terkait belum dipastikan [S66]
21 Nov 2026	**Kepolisian** Menolak klaim viral yang tidak didukung bukti mengenai gangguan global terkoordinasi yang berkepanjangan [S51]
21 Nov 2026	**SUB-ZER0** Mengiklankan dugaan materi verifikasi identitas dari platform yang tidak disebutkan namanya [S1]
22 Nov 2026	**AFKForever** Mengiklankan dugaan akses VPN perguruan tinggi pada hari batas pengamatan [S1]

Kronologi menempatkan kejadian publikasi berdampingan dengan kejadian publikasi lainnya. Jika sumber menjelaskan tanggal aktivitas yang lebih awal, entri menyatakan pembedaan tersebut. Entri bukan jumlah penyusupan yang berbeda.

Alias unggahan mengidentifikasi persona yang berkaitan dengan publikasi. Alias tidak mengidentifikasi orang yang mengoperasikan akun. Kronologi tidak menyiratkan koordinasi antar persona yang tercantum.

6.3 Bandingkan hal yang dibuktikan, bukan jumlah yang bersaing

Pokok	Klaim atau peringatan	Keterangan resmi	Penafsiran
Ancaman gangguan sistem publik	Ancaman yang beredar memicu perhatian terhadap kesiapsiagaan [S48]	Komdigi meneruskan koordinasi BSSN sementara keaslian dan kemampuan belum dipastikan [S48]	Persiapan didukung; serangan yang berhasil tidak dibuktikan oleh pemberitahuan ini

Pokok	Klaim atau peringatan	Keterangan resmi	Penafsiran
Dugaan akses saat ini	Persona mengiklankan akses terkait perbankan yang masih berfungsi [S1]	Sumber pendukung tidak memberikan konfirmasi resmi yang berkaitan	Akses saat ini, cakupan, dan hasilnya memerlukan validasi terpisah
Informasi yang beredar kembali	Unggahan saat ini dapat menyajikan data seolah-olah baru [S1]	Komdigi menjelaskan peredaran kembali informasi lama dalam materi yang dibahas pemberitahuan Oktober [S46]	Keterangan tersebut tidak memastikan status setiap penawaran atau setiap kumpulan data yang beredar saat ini
Ketersediaan platform pengembangan	Pengguna mengalami gangguan akses	Komdigi mengaitkan gangguan 6 November dengan pemblokiran IP bersama dan menjelaskan pemulihan [S47]	Dampak ketersediaan terkonfirmasi tidak membuktikan penyusupan platform
Gangguan layanan global	Gangguan layanan dapat menarik rumor serangan	BSSN meneruskan penjelasan proses yang kelebihan beban dan tidak adanya indikasi aktivitas berbahaya [S50]	Pemulihan operasional dan pertahanan terhadap phishing oportunistis tetap relevan
Narasi viral gangguan berkepanjangan	Klaim menyebut gangguan perbankan dan internet global selama berbulan-bulan	Polisi menyatakan tidak ada bukti pendukung yang kredibel [S51]	Rumor bukan insiden terverifikasi atau prakiraan

Panel klaim dan keterangan resmi tidak boleh memaksakan ukuran yang berbeda menjadi rasio. Jumlah permintaan, durasi, jumlah akun, dan jumlah sasaran yang diklaim pelaku menjawab pertanyaan berbeda.

Perbandingan yang tepat adalah apakah bukti mendukung suatu hal tertentu. Apakah layanan menurun? Apakah akses tanpa izin terjadi? Apakah informasi terpapar? Apakah operator yang disebut dalam klaim menyebabkan dampak yang diamati?

6.4 Bukti ketersediaan perlu mempertahankan dimensinya

Penanggung jawab layanan perlu mencatat awal penurunan, fungsi terdampak, dan waktu pemulihannya. Keterjangkauan eksternal dan alur pelanggan yang diautentikasi dapat berbeda. Respons halaman utama tidak membuktikan jalur transaksi berfungsi.

Untuk dugaan DDoS, penanggung jawab jaringan perlu membandingkan karakteristik permintaan, kejadian infrastruktur, dan dampak pengguna. Tangkapan layar pelaku tidak membuktikan durasi atau jangkauan geografis gangguan.

Untuk dugaan perubahan tampilan situs tanpa izin, penanggung jawab aplikasi perlu menyimpan konten yang berubah dan riwayat publikasi. Perubahan halaman yang terlihat tidak membuktikan pengambilan data. Perubahan itu juga tidak membuktikan bahwa pemulihan menghapus jalur akses.

Untuk peringatan terkait DNS, penanggung jawab perlu memeriksa catatan yang disahkan dan riwayat perubahannya. Jawaban berbeda yang diamati melalui satu layanan dapat memiliki beberapa penjelasan. Catatan insiden perlu mempertahankan hal yang benar-benar diamati.

6.5 Gangguan layanan membuka peluang penipuan

Penyampaian ulang resmi oleh Kemenkes CSIRT pada 13 November atas imbauan BSSN memperingatkan phishing oportunistis sambil meneruskan penjelasan gangguan yang tidak menunjukkan aktivitas berbahaya. Saran tersebut relevan meskipun gangguan layanan tersebut bukan serangan siber. [S50]

Tim dukungan perlu memelihara saluran yang disetujui untuk pembaruan gangguan dan petunjuk pemulihan. Pelanggan dan pegawai memerlukan cara membedakan bantuan resmi dari pesan yang meminta kredensial atau pemasangan perangkat lunak.

Operasi keamanan perlu meninjau laporan pesan pemulihan yang menipu. Organisasi tidak boleh mengklaim pesan tersebut menyebabkan kompromi tanpa bukti. Upaya yang terekam dan penyusupan akun yang berhasil tetap merupakan hasil berbeda.

6.6 Komunikasikan hal yang didukung catatan layanan

Pernyataan pertama dapat menyebut gangguan layanan, pembatasan untuk pelindungan, dan saluran pembaruan berikutnya. Pernyataan tidak harus memberikan nama pelaku, penyebab, atau perkiraan orang terdampak sebelum hal tersebut dipastikan.

Pernyataan berikutnya perlu menjelaskan fakta yang berubah. Jika serangan yang diklaim tidak berkaitan dengan gangguan terukur, organisasi perlu menyimpan kesimpulan itu beserta bukti pendukungnya.

Periode terkini menunjukkan nilai disiplin tersebut. Kesiapsiagaan, kejadian operasional, dan rumor dapat muncul berdekatan. Kedekatan waktu tidak membuktikan penyebab yang sama.

6.7 Akses teknologi berhak istimewa memerlukan tujuan yang sah

Publikasi kepolisian pada 18 November melaporkan pemberhentian karena pelanggaran etik terkait penggunaan teknologi penegakan hukum tanpa izin. Banding telah diajukan. Dugaan pidana terkait menyangkut penyadapan, akses ilegal, dan penghapusan data elektronik. Temuan etik tersebut bukan putusan pidana bersalah. [S66]

Penanggung jawab sistem berhak istimewa perlu meninjau hak akses yang sah, persetujuan, dan catatan audit. Pertanyaan kontrolnya adalah siapa yang dapat mengakses kemampuan sensitif dan cara memeriksa kesesuaian penggunaan dengan tujuan yang diizinkan. Keterangan tidak membuktikan hubungan dengan klaim penjual dalam laporan ini.

TEMUAN UTAMA

01

Bersiap berdasarkan peringatan kredibel tanpa menyatakan serangan telah terjadi

02

Bandingkan klaim dengan dampak layanan yang terukur

03

Sampaikan petunjuk pemulihan pelanggan melalui saluran yang diautentikasi

BAB 07

Pelaku ancaman dan hubungan

07

PERTANYAAN BAB INI

Hubungan antarpelaku mana yang memiliki bukti konkret, dan mana yang tetap menjadi hipotesis penerbit?

28

Label kelompok pemerasan dalam Ransompedia

7.1 Peta membedakan hubungan 70
7.2 Amaranth-Dragon merupakan aktivitas terdahulu yang diungkap pada 2026 72
7.3 Kronologi WinRAR mendukung verifikasi pembaruan keamanan 73
7.4 SilentDelivery secara eksplisit mencakup Indonesia pada 2026 74
7.5 Silver Fox menggabungkan konfigurasi negara dan temuan yang diamati 75
7.6 Pelaporan BlueMoon menambah kampanye bertarget yang terpisah 76
7.7 Atribusi dan tanggal aktivitas StrikeShark belum dipastikan 77
7.8 Label pemerasan menggambarkan ekosistem pencantuman yang terlihat 78
7.9 Perbandingan regional tetap merupakan perbandingan pencantuman 80
7.10 Persona tetap merupakan identitas publikasi 81

BAB 07

Pelaku ancaman dan hubungan

RINGKASAN

Lanskap pelaku menggabungkan persona penjual, label pemerasan, dan kampanye yang dilacak vendor. Kategori tersebut tidak dapat dipertukarkan. Ransompedia mencatat 28 label kelompok. Laporan vendor menyebut Indonesia dalam aktivitas bertarget dengan tanggal dan batas atribusi berbeda. Alat bersama, iklan serupa, atau penyebutan negara yang sama tidak membuktikan satu operator. Gunakan peta hubungan untuk menelusuri bukti setiap hubungan, lalu dasarkan pekerjaan pertahanan pada kemampuan yang diamati, bukan atribusi tanpa dukungan bukti.

7.1 Peta membedakan hubungan

Peta pelaku perlu menghubungkan persona dengan unggahannya, label pencantuman dengan pencantumannya, dan klaster vendor dengan aktivitas yang dijelaskan vendor. Setiap hubungan memiliki jenis bukti.

Alat yang sama dapat mendukung hubungan penggunaan alat. Hal itu tidak otomatis membuktikan kendali bersama. Judul berulang dapat mendukung kemiripan iklan. Hal itu tidak membuktikan berkas identik atau perpindahan yang telah selesai.

Karena itu, laporan menggunakan kategori hubungan yang jelas. Pengamatan dan klaim tetap dibedakan dari keterangan resmi dan penafsiran vendor. Hubungan tanpa bukti tidak ditampilkan sebagai garis yang tampak setara.

Unggahan sendiri Penyampaian ulang Pernyataan resmi Laporan publik Pengamatan kami

Amaranth-Dragon

pelaporan publik
Aktivitas terdahulu pada 2025 diungkap pada 2026 [S21] ↑

Check Point Research

pelaporan publik
Indonesia disebut secara eksplisit dalam SilentDelivery [S28] ↓

SilentDelivery

Silver Fox

pelaporan publik
Temuan RustSL di Indonesia [S29] ↑

Kaspersky

pelaporan publik
Publikasi dengan tanggal aktivitas yang belum dipastikan [S43] ↓

StrikeShark

Proofpoint

pelaporan publik
Penargetan dijelaskan sejak 3 September [S42] ↓

UNK_QuietRacket

Penawaran terkait perbankan B01

unggahan sendiri
Alias publikasi [S1] ↑

updap

unggahan sendiri
Alias publikasi; tidak ada klaim kesamaan kumpulan data [S1] ↓

Klaim data kejadian B09

sellingood

unggahan sendiri
Rangkaian iklan berulang [S1] ↓

Rangkaian akun B07

Ransompedia

data sendiri
Populasi pencantuman bertanggal [S2] ↓

74 pencantuman terkait pemerasan

Keterangan resmi

resmi
Keterangan pengendali dan polisi; batas khusus setiap kasus [S35][S36][S38][S44] ↓

Berkas kasus pengendali dan polisi J–M

Pemberitaan mengenai tanggapan resmi

pelaporan publik
Tanggapan resmi dalam pemberitaan dengan batas yang belum dipastikan [S40] [S41] ↓

Berkas kasus berdasarkan pemberitaan N–O

TIDAK ADA HUBUNGAN TERBUKTI DENGAN PELAKU LAIN

Jenis hubungan	Contoh yang didukung	Batas
Unggahan sendiri	Persona ke iklan yang disimpan [S1]	Identitas asli persona dan hasil yang diiklankan belum dipastikan
Data sendiri	Ransompedia ke pencantuman terkait pemerasan yang bertanggal [S2]	Pencantuman bukan penyusupan terverifikasi
Pernyataan resmi	Otoritas ke fakta yang dilaporkannya [S35][S36][S48]	Dugaan penyelidikan dan pemberitahuan kesiapan mempertahankan statusnya
Pelaporan publik	Klaster vendor ke kampanye yang dijelaskan [S21][S28][S29][S42][S43]	Atribusi merupakan penilaian penerbit
Model analitis	Hubungan yang diusulkan dengan alternatif yang dinyatakan	Bukan hubungan yang diamati secara independen

7.2 Amaranth-Dragon merupakan aktivitas terdahulu yang diungkap pada 2026

Publikasi asli Check Point pada 4 Februari 2026 menjelaskan kampanye Amaranth-Dragon terhadap sasaran pemerintah dan penegakan hukum di Asia Tenggara. Bagian Indonesia membahas 18 Agustus dan 5 September 2025. Operasi tersebut mendahului periode aktivitas laporan ini. [S21]

Publikasi tetap relevan bagi prioritas pembaruan keamanan dan deteksi. Publikasi tidak boleh menjadi bukti penyusupan baru di Indonesia pada Februari 2026. Pembedaan ini perlu muncul dalam judul, kronologi, dan ringkasan kartu kasus.

Check Point menyatakan 18 Agustus sebagai penggunaan pertama CVE-2025-8088 oleh klaster ini yang diamatinya. Kampanye Indonesia berikutnya menggunakan alat akses jarak jauh yang dikendalikan melalui Telegram. Penerbit menjelaskan ketidakpastian pengiriman awal sambil menduga lampiran email berbahaya. [S21]

Atribusinya juga memiliki batas. Check Point melaporkan tumpang tindih alat dengan APT41 dan menilai adanya kemungkinan hubungan atau sumber daya bersama. Laporan ini mengatribusikan penilaian itu kepada Check Point. Tumpang tindih tidak diperlakukan sebagai temuan resmi Indonesia.

Amaranth-Dragon

Klaster yang dilacak vendor | Check Point menilai kemungkinan hubungan dengan APT41

DI INDONESIA, 2026

4 Februari
Check Point menerbitkan laporan tentang aktivitas terdahulu yang melibatkan Indonesia pada Agustus dan September 2025. [S21]

SASARAN YANG DIKLAIM

Sasaran pemerintah dan penegakan hukum di kawasan, sebagaimana dijelaskan Check Point. Aktivitas Indonesia mendahului periode laporan. [S21]

DALAM LAPORAN PUBLIK

[S21] Laporan asli Februari 2026 menjelaskan operasi 2025 dan pengiriman awal yang belum pasti.

PENILAIAN KAMI

Gunakan laporan untuk validasi pembaruan keamanan alat arsip dan konteks terdahulu. Jangan menghitungnya sebagai insiden Indonesia baru pada 2026.

TINGKAT KEYAKINAN

Keyakinan tinggi pada publikasi dan tanggal terdahulu; hubungan dengan APT41 tetap merupakan penilaian penerbit.

7.3 Kronologi WinRAR mendukung verifikasi pembaruan keamanan

Catatan CVE menyebut Windows WinRAR hingga versi 7.12 terdampak CVE-2025-8088. Kerentanan menyangkut penelusuran jalur dalam arsip yang dirancang khusus dan dapat memungkinkan eksekusi kode arbitrer. Catatan diterbitkan pada 8 Agustus 2025. [S22][S24]

Vendor menyebut versi 7.13 sebagai rilis perbaikan, bertanggal 30 Juli 2025. Catatan rilisnya kemudian diperbarui pada 12 Agustus. Artinya, rilis perbaikan mendahului publikasi CVE dan operasi Amaranth pada 18 Agustus yang dilaporkan. [S25][S26]

Karena itu, penilaian respons pembaruan keamanan perlu memeriksa apakah komponen arsip Windows yang rentan tetap digunakan setelah versi perbaikan tersedia. Eksploitasi berikutnya tidak boleh disebut zero-day hanya karena kampanye cepat mengadopsinya.

Vendor juga menyebut komponen Windows RAR dan UnRAR yang terdampak. Versi Unix, Linux, dan Android berada di luar cakupan terdampak dalam imbauan. Inventaris pembaruan keamanan perlu mempertahankan pembedaan platform tersebut. [S25][S26]

Tonggak	Tanggal	Makna
Rilis perbaikan WinRAR 7.13	30 Juli 2025	Tanggal rilis vendor
Publikasi CVE	8 Agustus 2025	Catatan kerentanan yang diterbitkan
Riset asli ESET	11 Agustus 2025	Analisis teknis publik [S27]
Pembaruan catatan rilis vendor	12 Agustus 2025	Perubahan redaksi imbauan
Eksploitasi Amaranth pertama yang diamati Check Point	18 Agustus 2025	Pengamatan kampanye oleh penerbit
Publikasi Check Point	4 Februari 2026	Tanggal pengungkapan, bukan tanggal aktivitas

Tugas pertahanannya adalah inventarisasi dan validasi. Penanggung jawab endpoint perlu mengidentifikasi komponen Windows yang relevan, memastikan versi terpasang, dan meninjau aktivitas arsip mencurigakan jika paparannya memerlukan pemeriksaan.

Pembaruan yang berhasil tidak membuktikan bahwa eksploitasi sebelumnya tidak pernah terjadi. Sebaliknya, keberadaan versi lama tidak membuktikan eksploitasi. Hal-hal tersebut memerlukan bukti berbeda.

7.4 SilentDelivery secara eksplisit mencakup Indonesia pada 2026

Penyelidikan Check Point pada 10 November 2026 menjelaskan aktivitas SilentDelivery yang dilacak sejak awal 2026. Indonesia disebut di antara negara sasaran aktivitas watering hole yang selektif. Situs yang dijelaskan telah diubah untuk tujuan berbahaya berasal dari sektor pemerintah, pelayaran, TI, dan riset. [S28]

Penerbit menjelaskan peringatan sertifikat Chrome palsu dan program yang mengaku sebagai pemasang sertifikat. Rangkaian pengiriman mengarah ke SquadC atau varian SparrowDoor. Satu arsip phishing terkait yang diunggah ke layanan analisis dari Indonesia berbagi infrastruktur backdoor dengan rangkaian watering hole. [S28]

Bukti itu lebih kuat daripada penyebutan negara hanya dalam umpan. Namun, bukti tersebut tetap tidak memberikan daftar lengkap korban Indonesia atau membuktikan bahwa setiap pengunjung situs yang terdampak terinfeksi.

Penerbit menggunakan nama CopperDragon untuk hipotesis hubungan pemasok di antara beberapa klaster yang oleh Check Point dikaitkan dengan Tiongkok. Hal itu tetap merupakan hipotesis Check Point. Alat atau infrastruktur bersama tidak membuktikan satu operator pada ketiga klaster. [S28]

Bukti Indonesia didukung secara khusus oleh SilentDelivery. Aktivitas telekomunikasi klaster lain di Amerika Latin tidak boleh dipindahkan ke kasus Indonesia. Laporan global dapat memuat beberapa pengamatan dengan geografi berbeda.

SilentDelivery

Operasi yang dilacak vendor | Terhubung dengan hipotesis pemasok terkait Tiongkok CopperDragon, menurut Check Point

DI INDONESIA, 2026

Awal 2026
Check Point mulai melacak aktivitas watering hole yang selektif. [S28]

10 November
Laporan asli secara eksplisit menyebut Indonesia di antara negara sasaran. [S28]

SASARAN YANG DIKLAIM

Organisasi di Indonesia dan negara lain yang menggunakan situs sektor pemerintah, pelayaran, TI, dan riset, sebagaimana dijelaskan penerbit. [S28]

DALAM LAPORAN PUBLIK

[S28] Aktivitas watering hole dan phishing terkait mengirim varian SquadC atau SparrowDoor.

PENILAIAN KAMI

Check Point mengajukan hipotesis CopperDragon sebagai pemasok kerangka bersama bagi SilentDelivery dan dua klaster lainnya. Hipotesis calon pemasok tersebut mendukung hubungan penggunaan alat, bukan satu operator untuk seluruh klaster. [S28]

TINGKAT KEYAKINAN
Keyakinan tinggi pada pengamatan Indonesia yang dinyatakan penerbit; identitas pemasok dan kendali bersama tetap memiliki batas.

Bagi tim pertahanan, pertanyaan praktisnya menyangkut pemasangan perangkat lunak tak terduga setelah kunjungan ke situs tepercaya. Penanggung jawab endpoint dan dukungan browser perlu meninjau peluncuran pemasang, asalnya, dan aktivitas kendali jarak jauh terkait.

Panduan pengguna perlu menjelaskan jalur yang disetujui untuk masalah browser dan sertifikat. Tampilan situs tepercaya tidak mengesahkan permintaan pemasangan perangkat lunak. Proses dukungan perlu menyediakan saluran verifikasi yang mudah diakses.

7.5 Silver Fox menggabungkan konfigurasi negara dan temuan yang diamati

Laporan Kaspersky pada 30 April menjelaskan aktivitas bertema pajak dari Desember 2025 hingga awal 2026. Laporan secara eksplisit menyebut temuan RustSL di Indonesia. Indonesia ditempatkan di antara negara dengan serangan terbanyak yang diamati dalam telemetrinya. [S29]

Loader yang disesuaikan menyertakan Indonesia dalam daftar negara eksekusi. Telemetri nyata memberikan bukti yang terpisah dari konfigurasi. Negara yang tercantum dalam konfigurasi saja tidak membuktikan adanya temuan di negara tersebut.

Rangkaian menggunakan loader RustSL yang dimodifikasi dan ValleyRAT. Kaspersky juga menemukan plugin ValleyRAT yang memuat ABCDoor, backdoor yang penggunaannya mendahului 2026. Semua ini merupakan temuan dan penamaan penerbit. [S29]

Lebih dari 1,600 email berbahaya dalam laporan berkaitan dengan seluruh kampanye antara awal Januari dan awal Februari. Angka tersebut bukan jumlah Indonesia. Jumlah organisasi Indonesia maupun tanggal pertama yang tepat di Indonesia tidak diberikan.

Kaspersky mengatribusikan operasi kepada Silver Fox. Laporan ini tidak otomatis menggolongkan setiap tindakan yang dijelaskan sebagai spionase negara. Atribusi kampanye dan kemampuan yang diamati oleh sumber cukup untuk penilaian pertahanan.

Silver Fox

Kampanye yang diatribusikan vendor | Atribusi oleh Kaspersky

DI INDONESIA, 2026

Januari–Februari
Kaspersky menjelaskan aktivitas bertema pajak dan temuan RustSL di Indonesia. [S29]

30 April
Laporan asli menjelaskan ValleyRAT dan ABCDoor. [S29]

SASARAN YANG DIKLAIM

Pengguna Indonesia muncul dalam telemetri penerbit. Jumlah email seluruh kampanye bukan jumlah Indonesia. [S29]

DALAM LAPORAN PUBLIK

[S29] Publikasi asli membedakan konfigurasi negara dan temuan nyata.

PENILAIAN KAMI

Prioritaskan pengiriman dokumen mencurigakan dan aktivitas loader. Laporan tidak mengidentifikasi nama korban Indonesia atau membuktikan dukungan negara.

TINGKAT KEYAKINAN
Keyakinan tinggi pada publikasi dan temuan yang dilaporkan; cakupan pasti korban Indonesia belum dipastikan.

Prioritas kontrolnya adalah penanganan dokumen dan berkas eksekutabel dalam komunikasi yang tampak resmi. Penanggung jawab insiden perlu menelusuri rangkaian yang diamati sebelum menentukan apakah pengguna hanya menerima umpan atau menjalankan muatan berbahaya.

7.6 Pelaporan BlueMoon menambah kampanye bertarget yang terpisah

Laporan Proofpoint pada 9 September menjelaskan aktivitas UNK_QuietRacket yang menyasar pemerintah, konsultansi, dan keuangan di Indonesia dan Singapura sejak 3 September. Umpan terkait konferensi mengarah ke eksploitasi browser dan Windows yang dinamai BlueMoon oleh penerbit. [S42]

Proofpoint menilai adanya dugaan keterkaitan dengan Tiongkok. Itu merupakan penilaian penerbit, bukan atribusi laporan ini atau otoritas Indonesia. Keterangan pendukung tidak memastikan nama korban Indonesia.

Sumber juga menyatakan tidak ada muatan akhir yang diamati pada saluran perintah kedua. Rangkaian eksploitasi dan muatan akhir merupakan hal berbeda. Laporan mempertahankan batas itu tanpa melengkapi rangkaian berdasarkan asumsi.

UNK_QuietRacket

Aktivitas yang dilacak vendor | Dugaan keterkaitan dengan Tiongkok, menurut Proofpoint

DI INDONESIA, 2026

3 September

Proofpoint menyebut aktivitas bertarget yang melibatkan Indonesia dan Singapura dimulai pada tanggal ini. [S42]

9 September

Proofpoint menerbitkan analisis BlueMoon. [S42]

SASARAN YANG DIKLAIM

Pemerintah, konsultansi, dan keuangan di Indonesia dan Singapura, sebagaimana dinyatakan Proofpoint. [S42]

DALAM LAPORAN PUBLIK

[S42] Umpan konferensi dan eksploitasi browser/Windows dijelaskan; muatan akhir pada saluran kedua tidak diamati.

PENILAIAN KAMI

Tinjau urutan dari umpan hingga endpoint tanpa melengkapi bagian rangkaian yang belum diketahui berdasarkan asumsi.

TINGKAT KEYAKINAN

Keyakinan tinggi pada aktivitas yang dinyatakan penerbit; keterkaitan tetap merupakan penilaian penerbit.

Relevansi pertahanannya adalah undangan yang tampak tepercaya, diikuti perilaku browser atau endpoint yang tidak terduga. Tim email, endpoint, dan identitas perlu meninjau urutannya bersama. Pokok umpan tidak boleh menjadi bukti identitas operator.

7.7 Atribusi dan tanggal aktivitas StrikeShark belum dipastikan

Laporan Kaspersky pada 24 Juni menjelaskan aktivitas yang memengaruhi suatu entitas diplomatik yang berlokasi di Indonesia. Laporan mengaitkan layanan Exchange yang rentan dengan rangkaian SharkLoader dan Cobalt Strike, termasuk pengintaian sistem dan akses kredensial. [S43]

Keterangan pendukung tidak memberikan tanggal penyusupan yang pasti. Karena itu, publikasi dimasukkan dalam kronologi pelaporan. Publikasi tidak membuktikan penyusupan baru pada 24 Juni.

Kaspersky tidak mengatribusikan aktivitas dengan yakin kepada kelompok APT atau kriminal yang dikenal. Pengambilan data keluar tidak dibuktikan dalam bagian pendukung. Laporan tidak boleh menggantikan batas tersebut dengan label pelaku yang lebih dikenal.

StrikeShark

Aktivitas yang dinamai vendor | Tidak diatribusikan dalam riset pendukung

DI INDONESIA, 2026

24 Juni

Kaspersky menerbitkan laporan tentang aktivitas yang melibatkan suatu entitas diplomatik yang berlokasi di Indonesia. [S43]

SASARAN YANG DIKLAIM

Suatu entitas diplomatik yang berlokasi di Indonesia. Keterangan pendukung tidak memberikan tanggal penyusupan yang pasti. [S43]

DALAM LAPORAN PUBLIK

[S43] Riset menjelaskan layanan Exchange yang rentan, SharkLoader, Cobalt Strike, pengintaian sistem, dan akses kredensial.

PENILAIAN KAMI

Selidiki layanan kolaborasi terpapar yang relevan dan perilaku setelah akses. Jangan menyimpulkan pengambilan data keluar atau operator yang dikenal.

TINGKAT KEYAKINAN

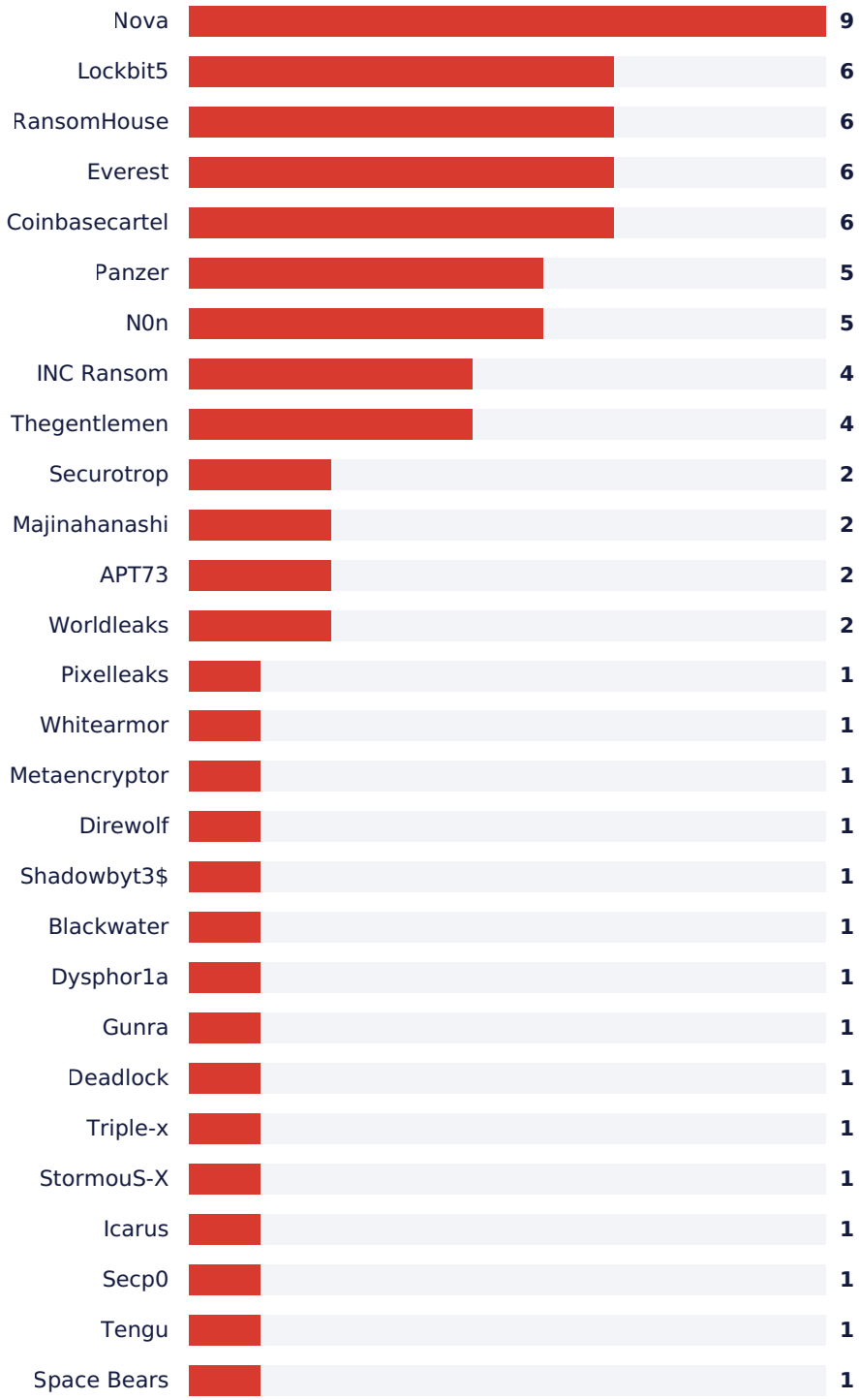
Keyakinan tinggi pada publikasi; tanggal aktivitas, atribusi kelompok yang dikenal, dan pengambilan data keluar belum dipastikan.

Implikasi operasionalnya menyangkut layanan kolaborasi yang terpapar dan aktivitas setelah akses. Penanggung jawab infrastruktur perlu memastikan penguatan layanan dan status pembaruan keamanan. Operasi keamanan perlu menyelidiki bukti pengintaian sistem dan akses kredensial yang relevan jika paparan atau kejadian memerlukannya.

7.8 Label pemerasan menggambarkan ekosistem pencantuman yang terlihat

Ransompedia mengaitkan 28 label dengan 74 pencantuman Indonesia. Nova mencakup sembilan. Lockbit5, RansomHouse, Everest, dan Coinbasecartel masing-masing mencakup enam. Panzer dan N0n masing-masing mencakup lima. [S2]

Pencantuman terkait pemerasan tersebar pada 28 label kelompok

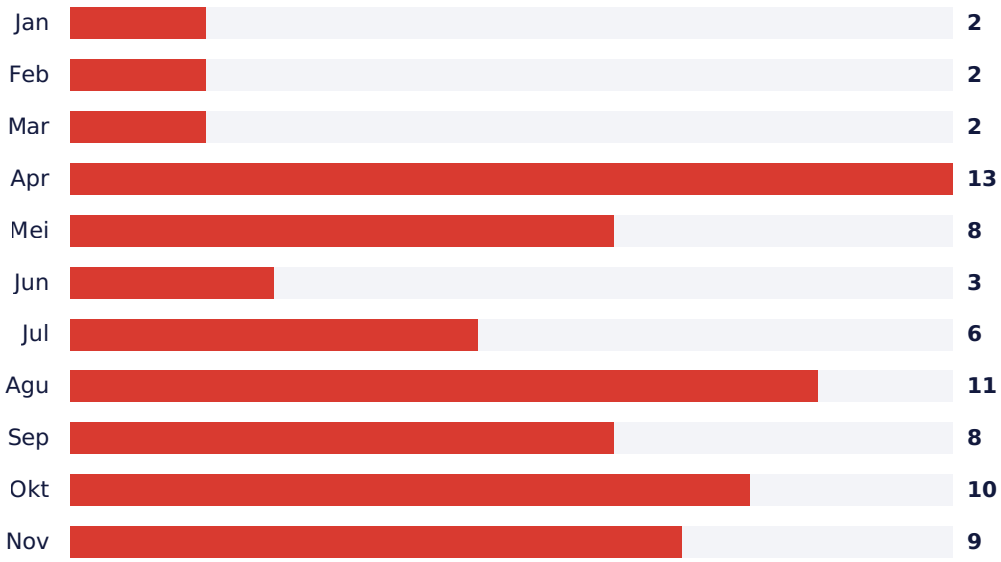


Sumber: pencantuman terkait pemerasan berlabel negara di Ransompedia, 1 Januari–22 November 2026; hari terakhir parsial [S2]. Klaim pencantuman bukan insiden terkonfirmasi, korban unik, atau penyusupan berhasil.

Label tersebut bukan jumlah operator independen yang terverifikasi. Nama dapat berubah, afiliasi dapat bertumpang tindih, dan pencantuman dapat memuat klaim yang belum terverifikasi. Laporan tidak menyimpulkan hubungan tersebut tanpa bukti pendukung.

November memuat sembilan pencantuman secara keseluruhan: tiga bertanggal 1 hingga 7 November dan enam dalam periode terkini dari 8 hingga 22 November. Enam pencantuman terkini melibatkan Panzer, N0n, INC Ransom, dan Pixelleaks. Publikasi terkini suatu label dapat mendasari pemantauan dan peninjauan kesinambungan. Hal itu tidak dapat mengidentifikasi teknik akses awal atau membuktikan bahwa enkripsi terjadi. [S2]

Tanggal pencantuman terkait pemerasan bervariasi selama periode pengamatan



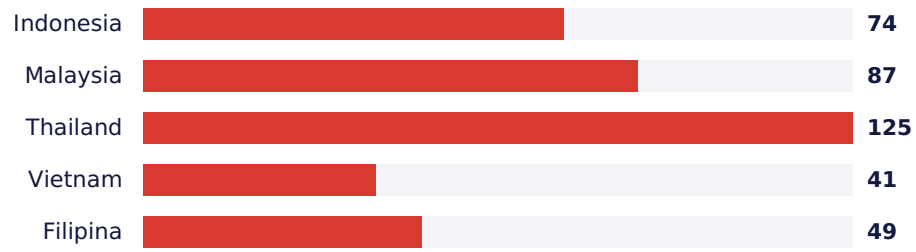
Sumber: pencantuman terkait pemerasan berlabel negara di Ransompedia, 1 Januari–22 November 2026; hari terakhir parsial [S2]. Klaim pencantuman bukan insiden terkonfirmasi, korban unik, atau penyusupan berhasil.

7.9 Perbandingan regional tetap merupakan perbandingan pencantuman

Label negara	Pencantuman dalam periode	Penafsiran yang diperbolehkan
Thailand	125	Jumlah pencantuman terbesar di antara lima label negara ini
Malaysia	87	Lebih banyak pencantuman yang diamati daripada Indonesia dalam periode yang sama
Indonesia	74	Populasi pencantuman Ransompedia yang terbatas
Filipina	49	Jumlah pencantuman yang diamati lebih kecil
Vietnam	41	Jumlah pencantuman yang diamati lebih kecil

Negara-negara pembanding dipilih sebagai contoh semata-mata untuk memberikan konteks; pemilihan tersebut tidak menyiratkan peringkat atau penilaian politik.

Label negara regional menunjukkan jumlah pencantuman yang berbeda



Sumber: pencantuman terkait pemerasan berlabel negara di Ransompedia, 1 Januari-22 November 2026; hari terakhir parsial [S2]. Klaim pencantuman bukan insiden terkonfirmasi, korban unik, atau penyusupan berhasil.

Perbandingan tidak memeringkat keamanan nasional atau tingkat insiden. Ekonomi, keterlihatan pelaporan, dan populasi organisasi berbeda. Jumlah pencantuman tidak boleh dinormalisasi menjadi probabilitas risiko tanpa penyebut yang sesuai. [S2]

Tindakannya adalah perencanaan dengan pembelajaran dari organisasi sejenis. Organisasi dapat memeriksa apakah pengaturan pemulihan, pemasok, dan notifikasinya menangani dampak yang dicontohkan di kawasan. Organisasi tidak boleh menyimpulkan bahwa jumlah pencantuman yang lebih rendah membuktikan paparan yang lebih rendah.

7.10 Persona tetap merupakan identitas publikasi

Korpus memuat penjual akses, pembeli dokumen, dan pengiklan akun. Perannya disimpulkan dari aktivitas yang dijelaskan dalam unggahan yang disimpan. Persona bukan identitas hukum atau anggota kelompok terorganisasi yang telah terbukti. [S1]

Alias berulang mendukung keterkaitan publikasi. Kesamaan bahasa atau harga penawaran serupa tidak mendukung penggabungan operator. Peta perlu mempertahankan simpul terpisah sampai bukti konkret mendukung hubungan.

updap

Persona publikasi | Identitas asli belum dipastikan

DI INDONESIA, 2026

17 Oktober
Iklan akses terkait perbankan, Kasus A. [B01]

12 November
Klaim data kejadian layanan teknologi, Kasus I. [B09]

SASARAN YANG DIKLAIM

Dua klaim mengenai peran layanan yang berbeda dikaitkan dengan alias publikasi. [S1]

DALAM KATA-KATA MEREKA

"This is not historical data. This is live production access right now." B01

DALAM LAPORAN PUBLIK

Bukti yang dikutip membuktikan publikasi yang disimpan, bukan atribusi eksternal.

PENILAIAN KAMI

Bukti yang dikutip membuktikan publikasi yang disimpan, bukan atribusi eksternal. [S1] Identitas publikasi yang sama tidak memastikan keaslian kedua klaim atau membuktikan kumpulan data berasal dari sumber yang sama.

TINGKAT KEYAKINAN
Keyakinan tinggi pada keterkaitan alias dengan unggahan; keaslian klaim dan identitas asli belum dipastikan.

sellingood

Persona rangkaian iklan | Identitas asli belum dipastikan

DI INDONESIA, 2026

Januari–Maret
Daftar penawaran harga per negara yang berulang untuk akun pesan. [B07]

SASARAN YANG DIKLAIM

Akun bernomor Indonesia diiklankan dalam daftar penawaran yang lebih luas. [S1]

DALAM KATA-KATA MEREKA

"Telegram Accounts for Sale - Desktop Tdata \ Session+Json Files" B07

DALAM LAPORAN PUBLIK

Bukti yang dikutip membuktikan publikasi yang disimpan, bukan atribusi eksternal.

PENILAIAN KAMI

Bukti yang dikutip membuktikan publikasi yang disimpan, bukan atribusi eksternal. [S1] Jangan menafsirkan pengulangan daftar penawaran sebagai pelanggaran keamanan tambahan atau menyimpulkan seluruh akun dicuri.

TINGKAT KEYAKINAN
Keyakinan tinggi pada iklan berulang; asal akun dan transaksi belum dipastikan.

TEKNIK YANG DIPETAKAN DARI PERILAKU DALAM RISET VENDOR, MENURUT TAKTIK

Akses awal
T1189 Kompromi melalui kunjungan situs
T1566.001 Lampiran spearphishing

Pemetaan analitis perilaku watering hole dan lampiran berbahaya yang dijelaskan vendor [S28][S29], menggunakan definisi MITRE [S85][S86]. Ini tidak membuktikan salah satu perilaku terjadi pada setiap sasaran Indonesia. [S85]

Tampilan ATT&CK terbatas memetakan perilaku watering hole ke T1189 dan lampiran berbahaya ke T1566.001 menggunakan definisi MITRE. [S85][S86]

Ini merupakan pemetaan analitis perilaku yang dijelaskan vendor. Pemetaan tidak membuktikan salah satu teknik terjadi pada setiap sasaran Indonesia. [S28][S29]

TEMUAN UTAMA

01
Atribusikan penilaian pelaku kepada penerbitnya

02
Bedakan penggunaan alat bersama dari kendali bersama

03
Gunakan kemampuan dan bukti saat ini untuk memilih pekerjaan pertahanan

BAB 08

Ekonomi penipuan

08

PERTANYAAN BAB INI

Bagaimana tim pertahanan merespons iklan mengenai akun, dokumen identitas, atau catatan pembayaran?

3

Hal yang berbeda: ketersediaan, perpindahan, dan penggunaan yang berhasil

8.1 Pasar menawarkan produk yang berbeda 85
8.2 Bukti dari sisi permintaan memiliki makna berbeda 85
8.3 Sesi yang dapat dipindahtangankan memerlukan peninjauan keamanan akun 86
8.4 Klaim verifikasi identitas tidak memastikan keaslian platform 86
8.5 Harga penawaran mempertahankan satuan yang diiklankan 87
8.6 Catatan kartu pembayaran memerlukan cakupan sempit 87
8.7 Pelaporan penegakan hukum memerlukan batas periode tersendiri 87
8.8 Operasional penanganan penipuan perlu mempertahankan jejak keputusan 88

BAB 08

Ekonomi penipuan

RINGKASAN

Korpus yang disimpan memuat permintaan dokumen identitas, iklan akun pesan, dan dugaan materi verifikasi identitas. Pengamatan tersebut menggambarkan penawaran komersial. Pengamatan tidak membuktikan perpindahan dokumen, penjualan selesai, atau verifikasi berhasil. Angka kartu pembayaran memiliki populasi lebih sempit dan tidak dapat mengukur pencurian atau kerugian nasional. Tim antipenipuan perlu menghubungkan setiap penawaran relevan dengan bukti internal akun, pendaftaran, dan transaksi, lalu mendokumentasikan apakah kemampuan yang diiklankan menimbulkan risiko saat ini bagi pelanggan atau usaha.

8.1 Pasar menawarkan produk yang berbeda

Permintaan dokumen identitas, akun yang dapat dipindahtangankan, dan penawaran data menimbulkan tugas verifikasi berbeda. Pembeli dapat mencari bukti organisasi nyata. Penjual akun dapat menawarkan akun baru atau sesi yang dapat digunakan kembali. Penjual data dapat mengiklankan materi lama. [S1]

Alternatif itu penting karena harga saja tidak dapat mengidentifikasi asal. Harga penawaran rendah tidak membuktikan kompromi massal. Harga tinggi tidak membuktikan akses berhak istimewa atau populasi pelanggan yang diautentikasi.

Kasus korpus mempertahankan satuan yang diiklankan. Catatan tetap menjadi catatan, kejadian tetap menjadi kejadian, dan akun tetap menjadi akun. Jumlahnya tidak berubah menjadi orang unik tanpa bukti pendukung.

8.2 Bukti dari sisi permintaan memiliki makna berbeda

Permintaan pembelian dokumen pada Maret mencari dokumen identitas dan pendaftaran usaha Indonesia untuk perusahaan aktif. Permintaan menyebut materi asli yang belum kedaluwarsa serta menolak dokumen yang diedit atau palsu. Hal itu membuktikan permintaan yang dinyatakan pembeli. [S1]

Hal itu tidak membuktikan tanggapan pemasok, perpindahan, verifikasi berhasil, atau kendali perusahaan. Tujuan penggunaan berikutnya belum dipastikan. Laporan tidak menyimpulkan penipuan yang telah dilakukan dari permintaan tersebut.

Bagi tim penerimaan pelanggan, implikasi perencanaannya menyangkut kewenangan selain tampilan dokumen. Dokumen dapat merujuk orang atau usaha nyata tanpa membuktikan bahwa pemohon berhak mewakilinya.

Karena itu, uji penyelesaian perlu menggabungkan bukti identitas dengan pemeriksaan hubungan saat ini. Penanggung jawab bisnis perlu mencatat pemberi kewenangan kepada pemohon, kontak independen yang mengonfirmasi hubungan, dan kesesuaian permintaan dengan aktivitas yang diharapkan.

8.3 Sesi yang dapat dipindahtangankan memerlukan peninjauan keamanan akun

Rangkaian iklan akun pesan menawarkan akun bernomor Indonesia dan format materi akun yang dapat digunakan kembali. Alias yang sama mengiklankan $0.45 pada Januari dan $0.40 menjelang akhir Februari atau Maret. Penjual terpisah pada Juli dan November juga mengiklankan materi akun. Daftar penawaran November menyebut akun baru dan lama atau format sesi yang dapat digunakan kembali. [S1]

Angka tersebut merupakan harga penawaran dalam unggahan tertentu. Angka itu tidak membuktikan harga pasar umum atau penurunan biaya akun curian. Akun mungkin baru didaftarkan, bukan diambil dari pengguna yang sudah ada.

Rangkaian berulang mendukung peredaran sepanjang waktu. Rangkaian itu tidak membuktikan pelanggaran keamanan tambahan setiap kali daftar penawaran yang sama muncul kembali. Rangkaian juga tidak menghubungkan setiap penjual dengan deskripsi serupa.

Tim keamanan dan antipenipuan perlu meninjau pendaftaran akun, otomatisasi, dan perilaku sesi yang relevan. Organisasi perlu membedakan upaya masuk, sesi yang disahkan, dan penggunaan tanpa izin.

Perubahan kata sandi saja tidak menjelaskan keadaan sesi. Jika bukti internal membuktikan akses tanpa izin, penanggung jawab identitas perlu menentukan perlunya pencabutan sesi, perubahan pemulihan, atau peninjauan token integrasi.

8.4 Klaim verifikasi identitas tidak memastikan keaslian platform

Penawaran verifikasi identitas terkini menjelaskan lebih dari satu juta entri, atribut identitas, dan foto swafoto. Penawaran menyembunyikan platform yang diduga serta mengklaim penerimaan data masih berlangsung. Itu merupakan pernyataan penjual, bukan kondisi operasional yang terverifikasi. [S1]

Daftar skema dapat menggambarkan jenis data yang masuk akal tanpa membuktikan keaslian. Daftar tidak mengidentifikasi pengendali, membuktikan sumber, atau menunjukkan bahwa setiap catatan yang diiklankan unik.

Perhatian pertahanan yang tepat adalah penggunaan ulang identitas dan penyamaran. Penanggung jawab pencegahan penipuan perlu mencari penggunaan identitas berulang, hubungan akun yang tidak lazim, serta ketidakcocokan dokumen dan perilaku pemohon saat ini. Ini merupakan pemeriksaan yang dianjurkan, bukan hasil penipuan yang diamati.

Tim privasi dan pelanggan perlu menghindari penamaan platform berdasarkan deskripsi data yang luas. Atribusi yang salah dapat mengarahkan pelindungan ke sasaran keliru dan merugikan organisasi yang tidak terlibat.

8.5 Harga penawaran mempertahankan satuan yang diiklankan

Barang yang diiklankan	Ketentuan harga yang diamati	Hal yang belum dipastikan
Akses jarak jauh sektor pertanian	$1,000	Akses saat ini, hak yang dinyatakan, dan penjualan selesai
Data dan akses layanan pendapatan	$3,500	Keaslian, identitas berkas, hak saat ini, dan transaksi
Dokumen identitas dan usaha	$100 per set, dengan ketentuan perantara	Pasokan, perpindahan, tujuan, dan penggunaan berhasil
Akun pesan bernomor Indonesia	$0.45 pada Januari; $0.40 dalam unggahan berikutnya	Asal, kualitas akun, dan pembelian selesai
Akses jarak jauh perguruan tinggi	984,312 satoshi	Keabsahan akses, hak, jumlah host, dan penjualan

Tabel mempertahankan mata uang dan satuan setiap unggahan. Jumlah satoshi tidak dikonversi menjadi mata uang fiat, dan produk berbeda tidak dibandingkan sebagai indeks harga. [S1]

8.6 Catatan kartu pembayaran memerlukan cakupan sempit

CAKUPAN ANGKA KARTU

Angka kartu pembayaran mencakup catatan kartu pembayaran dalam korpus unggahan yang disimpan. Angka tersebut tidak mengukur paparan nasional, pencurian kartu, atau kerugian penipuan.

Tiga catatan kartu pembayaran yang terkait dengan Indonesia muncul dalam tiga unggahan yang disimpan. Angka tersebut merupakan jumlah catatan dan unggahan. Tim keuangan perlu memvalidasi hubungan akun atau pelanggan yang relevan melalui bukti internal yang sah sebelum menentukan tindakan pelindungan. [S1]

8.7 Pelaporan penegakan hukum memerlukan batas periode tersendiri

Keterangan polisi pada April menjelaskan penyelidikan alat phishing yang dikoordinasikan secara internasional, termasuk 22 alat dan dua penangkapan. Keterangan publik juga membahas korban lintas negara dan kerugian dari Januari 2023 hingga April 2024. [S57]

Pengumuman penegakan hukum pada 2026 tidak memindahkan korban terdahulu ke populasi insiden Indonesia tahun ini. Penangkapan juga berbeda dari putusan bersalah. Laporan menggunakan keterangan tersebut untuk menggambarkan pasar alat dan respons penegakan hukum.

Pelajaran pertahanannya adalah memisahkan perolehan, upaya penggunaan, dan dampak yang berhasil terjadi. Alat yang ditawarkan tidak membuktikan penggunaannya terhadap organisasi tertentu. Pelanggan yang menerima umpan tidak membuktikan kehilangan kredensial.

8.8 Operasional penanganan penipuan perlu mempertahankan jejak keputusan

Tim antipenipuan dan keamanan perlu berbagi bukti tanpa menggabungkan hasilnya. Penyelidikan keamanan dapat membuktikan akses tanpa izin, sementara peninjauan transaksi membuktikan apakah uang berpindah. Analisis privasi dapat membuktikan dampak data yang berbeda.

Penanggung jawab insiden perlu mencatat setiap kesimpulan dan dasarnya. Catatan perlu membedakan hasil berupa upaya, pemblokiran, aktivitas tanpa izin, dan kerugian terkonfirmasi. Catatan juga perlu mempertahankan periode yang relevan.

Struktur ini mendukung pelindungan pelanggan tanpa melebihkan bukti pasar. Struktur memperjelas tindakan berikutnya dan memungkinkan fakta berikutnya mengubah penilaian.

TEMUAN UTAMA

01

Pertahankan satuan yang diiklankan dan status sebagai harga penawaran

02

Validasi kewenangan pemohon selain tampilan dokumen

03

Hubungkan sinyal catatan pembayaran dengan bukti internal saat ini

BAB 09

Perbankan dan jasa keuangan

09

PERTANYAAN BAB INI

Bagaimana lembaga keuangan menggabungkan klaim akses, bukti transaksi, dan kesinambungan layanan?

2

Hasil yang terpisah: akses tanpa izin dan kerugian keuangan

9.1 Empat pertanyaan perlu tetap dipisahkan 90
9.2 Iklan perbankan memiliki klaim terbatas 90
9.3 Bukti transaksi perlu mendasari pernyataan kerugian keuangan 91
9.4 Informasi pelanggan dapat menimbulkan kewajiban paralel 91
9.5 Pembatasan layanan memerlukan perencanaan kesinambungan 91
9.6 Paparan sektor keuangan terpilih 92
9.7 Panduan sektor melengkapi respons insiden 92
9.8 Kesiapan pelaporan perlu dimulai dari keberlakuan 93
9.9 Insiden keuangan memerlukan penutupan bersama 93

BAB 09

Perbankan dan jasa keuangan

RINGKASAN

Jasa keuangan menghadapi pertanyaan berbeda mengenai identitas, keutuhan transaksi, data pelanggan, dan ketersediaan. Keterangan polisi mengenai bank daerah menjelaskan kerugian dan penyelidikan. Iklan terkait perbankan yang disimpan membuktikan klaim penjual mengenai beberapa sistem. Keduanya tidak boleh mengisi fakta yang belum tersedia pada keterangan lainnya. Lembaga perlu memvalidasi akses saat ini, merekonsiliasi aktivitas keuangan, dan mempertahankan penghitungan waktu pelaporan sesuai cakupan. Satukan pemimpin insiden, penanggung jawab kejahatan keuangan, layanan, dan privasi dalam satu catatan fakta.

9.1 Empat pertanyaan perlu tetap dipisahkan

Lembaga keuangan perlu menanyakan apakah akses tanpa izin terjadi, informasi terpapar, transaksi berubah, dan ketersediaan layanan menurun. Bukti untuk satu hal tidak membuktikan keempatnya.

Backend yang diiklankan merupakan petunjuk mengenai akses. Anomali transaksi merupakan petunjuk mengenai aktivitas keuangan. Keluhan pelanggan dapat menyangkut keduanya, sementara gangguan layanan dapat timbul dari pembatasan untuk pelindungan atau penyebab lain.

Kasus bank daerah menunjukkan pentingnya mempertemukan jalur tersebut. Polisi menjelaskan penyusupan sistem pada Februari dan kerugian akun. Pelaporan awal menjelaskan pembatasan akses digital dan audit forensik. Masing-masing merupakan tonggak kasus yang berbeda. [S36][S37]

Pemimpin penanganan insiden perlu mengoordinasikan jalur tersebut. Tim kejahatan keuangan memvalidasi transaksi. Penanggung jawab identitas memvalidasi akun dan sesi. Penanggung jawab aplikasi menentukan izin layanan. Tim privasi menilai informasi yang terlibat.

9.2 Iklan perbankan memiliki klaim terbatas

Unggahan 17 Oktober mengiklankan dugaan akses backend mobile banking beserta basis data API promosi. Unggahan mengklaim informasi pelanggan dan administrator serta menyebut akses masih berlaku. Pernyataan tersebut tetap merupakan dugaan penjual. [S1]

Adanya istilah perbankan tidak membuktikan seluruh sistem yang dijelaskan berbagi batas kepercayaan. Infrastruktur promosi dan layanan inti pelanggan dapat memiliki izin serta operator berbeda. Penyelidikan perlu menentukan hubungan sebenarnya.

Pembedaan ini mencegah klaim akses berubah menjadi kesimpulan kompromi seluruh bank. Pembedaan juga menghindari pengabaian masalah sistem promosi hanya karena sistem inti tidak terdampak.

Validasi pertama perlu mengidentifikasi layanan yang dikelola dan kejadian autentikasi yang relevan. Penanggung jawab kemudian perlu menilai izin dan informasi sensitif yang dikembalikan. Sesi tanpa izin yang masih aktif mendasari respons berbeda dari deskripsi layanan yang belum terverifikasi.

9.3 Bukti transaksi perlu mendasari pernyataan kerugian keuangan

Polisi melaporkan transfer dari rekening milik 6,609 nasabah dan sekitar Rp144 miliar kerugian dalam penyelidikan bank daerah. Angka ini menggambarkan skala yang dilaporkan dalam penyelidikan. Angka nasabah tidak membuktikan jumlah rekening terdampak. [S36]

Keterangan yang sama menjelaskan aset yang dibekukan selama penyelidikan. Jumlah yang dibekukan tidak otomatis merupakan jumlah yang dipulihkan atau diganti kepada pelanggan. Pimpinan perlu meminta catatan keuangan terpisah untuk setiap hasil.

Operasional pelanggan juga perlu membedakan keluhan yang dilaporkan dari transaksi tanpa izin yang tervalidasi. Keluhan memerlukan penanganan segera, tetapi lembaga perlu mempertahankan status klaim yang mendasarinya.

Penanggung jawab keuangan perlu memelihara rekonsiliasi yang menghubungkan transaksi, akun, penanda waktu, dan keputusan penanganan kasus. Pernyataan publik perlu menjelaskan hanya satuan dan status yang didukung rekonsiliasi itu.

9.4 Informasi pelanggan dapat menimbulkan kewajiban paralel

Kejadian akses dapat melibatkan informasi profil tanpa manipulasi pembayaran terkonfirmasi. Kejadian transaksi juga dapat memerlukan penyelidikan saat cakupan data belum diketahui. Catatan insiden perlu mendukung kedua analisis.

Pengungkapan platform konsumen menggambarkan pembatasan sesuai jenis data. Populasi akun sementara yang disebut pengendali berbeda dari informasi yang terdampak bagi setiap pengguna. Pengecualian yang dilaporkan harus tetap diatribusikan, bukan diubah menjadi temuan forensik independen. [S44]

Lembaga keuangan perlu menyiapkan pesan pelanggan dengan batas serupa. Pesan perlu menyebut layanan, dampak yang diketahui, dan jalur dukungan resmi. Pesan perlu menghindari pengaitan penawaran yang tidak terkait atau jaminan tiadanya penyalahgunaan mendatang hanya karena belum diamati.

Tim privasi perlu mendokumentasikan hal yang diketahui pada setiap keputusan notifikasi. Perubahan berikutnya perlu diperlakukan sebagai pembaruan kasus yang sama jika kejadian dasarnya sama.

9.5 Pembatasan layanan memerlukan perencanaan kesinambungan

Pembatasan untuk pelindungan dapat mengurangi akses selama penyelidikan berlanjut. Dalam keterangan awal bank daerah, akses digital dibatasi sementara kantor cabang tetap tersedia. Itu merupakan pengamatan status layanan, bukan bukti seluruh saluran alternatif memenuhi setiap kebutuhan pelanggan. [S37]

Karena itu, perencanaan kesinambungan perlu menguji alur layanan pelanggan yang kritis. Pilihan pengganti dapat berfungsi untuk satu tugas pembayaran atau dukungan, tetapi gagal untuk tugas lain. Penanggung jawab layanan perlu mencatat alur yang diuji dan batasnya.

Komunikasi perlu menjelaskan cara pelanggan memperoleh bantuan yang diautentikasi. Tim antipenipuan perlu memantau penyamaran identitas lembaga selama gangguan. Tim keamanan perlu mencatat upaya penyalahgunaan secara terpisah dari transaksi berhasil.

9.6 Paparan sektor keuangan terpilih

Seluruh 25 domain perbankan dan keuangan memiliki keterkaitan perangkat dan catatan kredensial. Keterkaitan perangkat pegawai teramati pada 24, dan 10 memiliki kredensial diiklankan untuk dijual saat diperiksa. Jumlah sektor ini tidak membuktikan akses saat ini ke infrastruktur bank. [S4]

Portofolio perbankan dan keuangan mencakup sedikitnya 110,475 keterkaitan perangkat, termasuk 2,471 keterkaitan perangkat pegawai, dan 355,135 keterkaitan catatan kredensial. Portofolio juga mencakup 395 keterkaitan dokumen dan 5,072 pengamatan domain serupa dalam 30 hari sebelumnya. Populasi ini bertumpang tindih. [S4]

Perbankan dan keuangan memiliki pengamatan untuk 22 dari 25 domain kandidat. Kebijakan DMARC quarantine/reject teramati pada 19. Status TLS valid pada 18, tidak valid pada 1, dan tidak tersedia pada 3; pengamatan HTTP mencakup 10. [S3]

Asuransi dan jasa keuangan memiliki pengamatan untuk 24 dari 25 domain kandidat. Kebijakan DMARC quarantine/reject teramati pada 20. Status TLS valid pada 20, tidak valid pada 1, dan tidak tersedia pada 3; pengamatan HTTP mencakup 12. [S3]

Pengamatan kebijakan ini tidak membuktikan penerapan penuh pada pengiriman pesan. Jumlah header menggunakan cakupan HTTP masing-masing sektor, bukan penyebut TLS atau domain terpilihnya.

Portofolio sektor keuangan terpilih bukan seluruh industri keuangan. Jumlah kontrol yang dilaporkan perlu mempertahankan penyebut yang dinilai dan tanggal pengamatan. Peringkat Atlas sektoral tidak disajikan.

Keterkaitan kredensial tidak otomatis mengidentifikasi pegawai. Penanggung jawab identitas perlu menentukan hubungan dan keabsahan saat ini. Rujukan domain bank dalam unggahan juga bukan bukti bahwa infrastruktur bank sendiri telah diakses.

Angka kartu pembayaran mempertahankan cakupan sempit dalam Bab 8. Angka menyangkut catatan kartu pembayaran dalam korpus unggahan yang disimpan. Angka tidak mengukur paparan, pencurian, atau kerugian nasional.

9.7 Panduan sektor melengkapi respons insiden

OJK dan BSSN mengadakan lokakarya April bagi penyelenggara keuangan digital, mencakup kesiapsiagaan, deteksi, respons, dan pemulihan. Keterangan OJK pada November menjelaskan panduan ketahanan siber untuk pendanaan digital. Perkembangan ini bersifat pencegahan dan peningkatan kapasitas. [S52][S53]

Kegiatan tersebut tidak boleh dihitung sebagai insiden yang memengaruhi peserta. Nilai operasionalnya terletak pada fungsi yang dapat diuji lembaga: tanggung jawab yang jelas, deteksi insiden, respons terkendali, dan kemampuan pemulihan.

Lembaga keuangan perlu mengaitkan panduan tersebut dengan daftar layanannya sendiri. Daftar perlu mengidentifikasi aktivitas yang diatur, ketergantungan eksternal, informasi kritis, dan penerima pelaporan.

9.8 Kesiapan pelaporan perlu dimulai dari keberlakuan

Pelaporan siber bank umum menurut SEOJK 29/2022 mencakup notifikasi awal dalam 24 jam setelah bank mengetahui insiden. Laporan lebih lengkap harus disampaikan dalam lima hari kerja setelah diketahui. [S15]

Kerangka BI dalam cakupannya menggunakan satu jam setelah mengetahui insiden untuk notifikasi awal siber. Laporan lebih lengkap harus disampaikan dalam tiga hari kalender setelah kejadian. Lembaga harus mempertahankan perbedaan pemicu tersebut, bukan menggantinya dengan satu penanda waktu bersama. [S18]

Jika otoritas lain mensyaratkan pelaporan lebih cepat, surat edaran OJK memuat ketentuan pelaporan bersamaan. Penanggung jawab hukum dan kepatuhan perlu mengidentifikasi kewajiban yang bertumpang tindih sebelum insiden. Pemimpin penanganan insiden perlu menyediakan satu catatan fakta bersama. [S15]

9.9 Insiden keuangan memerlukan penutupan bersama

Bidang pekerjaan	Penanggung jawab	Pertanyaan penutupan
Identitas	Operasi identitas	Apakah akun, sesi, dan izin yang relevan telah divalidasi?
Transaksi	Tim kejahatan keuangan dan keuangan	Apakah perpindahan yang diperselisihkan telah direkonsiliasi dan hasil pelanggan dicatat?
Aplikasi	Penanggung jawab layanan	Apakah fungsi terdampak telah pulih dan jalur akses ditangani?
Data	Penanggung jawab privasi dan data	Apakah cakupan informasi telah dinilai dan diperbarui?
Pelaporan	Hukum dan kepatuhan	Apakah penerima yang berlaku diberi notifikasi dengan penghitungan waktu yang benar?
Pelanggan	Operasional pelanggan	Apakah dukungan yang diautentikasi dan petunjuk pelindungan tersedia?
Pemulihan	Penanggung jawab kesinambungan	Apakah layanan pengganti atau layanan yang dipulihkan telah diuji?

Kasus tidak boleh ditutup karena satu bidang pekerjaan selesai lebih dahulu. Rekonsiliasi transaksi dapat berlanjut setelah pembatasan teknis. Pemulihan bagi pelanggan dapat berlanjut setelah layanan pulih.

Penanggung jawab eksekutif perlu menerima status terpisah untuk hasil tersebut. Hal ini mendukung pelaporan kemajuan yang terbuka, tanpa menjadikan situs pulih atau akun nonaktif sebagai pengganti pemulihan lengkap.

TEMUAN UTAMA

01

Pisahkan temuan akses, data, transaksi, dan ketersediaan

02

Rekonsiliasi kerugian yang dilaporkan dan hasil pelanggan sesuai satuannya

03

Siapkan jalur pelaporan sesuai cakupan sebelum insiden

BAB 10

Respons regulasi

10

PERTANYAAN BAB INI

Kewajiban pelaporan apa yang berlaku bagi kegagalan data pribadi atau insiden siber, dan bagaimana pemicunya berbeda?

3 × 24 jam

Jangka waktu pemberitahuan tertulis menurut UU PDP dalam keadaan yang disebutkan

10.1 Kewajiban PDP sudah terdapat dalam undang-undang 96
10.2 Sanksi administratif merupakan batas hukum 96
10.3 PP 33/2026 memiliki tanggal berlaku mendatang 97
10.4 Pembentukan lembaga tetap merupakan pertanyaan status pada waktu tertentu 97
10.5 Pelaporan IIV memiliki jalur organisasi yang ditetapkan 98
10.6 Pelaporan siber bank umum tetap terpisah 98
10.7 Pelaporan BI menggunakan jangka waktu awal yang lebih singkat 99
10.8 Catatan bersama dapat mendukung penghitungan waktu yang berbeda 99
10.9 Latih bukti yang diperlukan untuk notifikasi 100

BAB 10

Respons regulasi

RINGKASAN

Kerangka Indonesia menggabungkan UU PDP, pengaturan IIV, dan aturan khusus sektor keuangan. Tenggatnya memiliki penerima dan pemicu berbeda. PP 33/2026 diterbitkan pada 2026. Keterangan resmi menyebut 16 Januari 2027 sebagai tanggal mulai berlakunya. Pernyataan pembentukan lembaga tetap memiliki tanggal dan batas. Penanggung jawab hukum dan operasional perlu memetakan kewajiban yang berlaku bagi setiap layanan, menyimpan bukti kejadian serta penemuan, dan melatih notifikasi beserta tanda terima pengirimannya.

10.1 Kewajiban PDP sudah terdapat dalam undang-undang

UU 27/2022 tentang Pelindungan Data Pribadi ditetapkan dan diundangkan pada 17 Oktober 2022. Catatan resmi BPK mencantumkannya sebagai berlaku. Asalnya pada 2022 tidak boleh mengaburkan relevansinya bagi keputusan insiden pada 2026. [S5]

Pasal 46 mewajibkan pengendali memberikan pemberitahuan tertulis dalam 3 × 24 jam ketika terjadi kegagalan pelindungan data pribadi. Penerimanya adalah subjek data dan lembaga. [S6]

Pemberitahuan setidaknya harus memuat data pribadi yang terungkap, waktu dan cara pengungkapan, serta upaya penanganan dan pemulihan oleh pengendali. Dalam keadaan tertentu, pengendali juga harus memberi tahu masyarakat. [S6]

Redaksi asli pasal tidak secara tegas menyebut "setelah penemuan". Laporan mempertahankan redaksi undang-undang tersebut. Penanggung jawab hukum perlu menentukan pemicu yang berlaku dan ketentuan tambahan dari teks hukum yang relevan.

Kejadian siber dan kegagalan data pribadi bukan label yang dapat dipertukarkan. Tim insiden perlu mengumpulkan fakta untuk memungkinkan penanggung jawab privasi dan hukum menilai kondisi dalam undang-undang. Penyimpanan bukti tidak boleh ditunda selama perdebatan istilah.

10.2 Sanksi administratif merupakan batas hukum

Pasal 57 mengatur peringatan tertulis, penghentian sementara pemrosesan, penghapusan atau pemusnahan data pribadi, dan denda administratif. Pasal tersebut memberikan kewenangan pengenaan sanksi kepada lembaga. [S6]

Batas denda adalah dua persen pendapatan tahunan atau penerimaan tahunan, dengan mempertimbangkan variabel pelanggaran. Itu merupakan batas dalam undang-undang. Laporan tidak menyebutnya denda otomatis setiap insiden atau kerugian keuangan yang terukur.

Keberadaan batas tidak membuktikan organisasi tertentu telah dinyatakan bertanggung jawab. Dalam kasus platform pelanggan, keterangan pendukung November menyatakan pemeriksaan berlanjut dan tanggung jawab atau sanksi belum ditentukan. [S45]

Karena itu, pimpinan perlu memisahkan respons insiden dari tanggung jawab yang telah diputuskan. Tindakan pelindungan dapat diperlukan sebelum penetapan kesalahan. Kesimpulan hukum akhir memerlukan kewenangan dan buktinya sendiri.

10.3 PP 33/2026 memiliki tanggal berlaku mendatang

Keterangan BPOM pada 15 September menyebut PP 33/2026 diundangkan pada 16 Juli 2026. Keterangan resmi Gianyar menyebutnya peraturan pelaksana UU 27/2022 dan menjelaskan periode enam bulan sebelum berlaku. [S7][S8]

Keterangan Bawaslu pada 12 November menyebut tanggal berlaku 16 Januari 2027. Pernyataan waktu yang tepat adalah bahwa peraturan pelaksana diterbitkan pada 2026 dengan tanggal berlaku mendatang. [S9]

Menyebut peraturan tersebut masih belum ada merupakan hal yang tidak tepat. Menyebutnya sudah berlaku pada batas pengamatan 22 November juga tidak tepat. Organisasi dapat mempersiapkan peraturan yang akan berlaku tanpa menyatukan tanggal-tanggal tersebut.

Persiapan perlu menghubungkan ketentuan hukum dengan alur data nyata. Penanggung jawab privasi perlu mengidentifikasi pengendali, prosesor, kategori data, dan layanan berdampak tinggi. Penanggung jawab aplikasi perlu memastikan bentuk hubungan tersebut dalam produksi.

Tim hukum perlu mencatat teks dan versi yang berlaku untuk setiap kewajiban. Materi pelatihan dan keterangan kegiatan dapat menjelaskan perkembangan. Namun, keduanya tidak boleh menggantikan aturan berwenang saat menentukan ketentuan prosedural terperinci.

10.4 Pembentukan lembaga tetap merupakan pertanyaan status pada waktu tertentu

Pasal 58 menyatakan lembaga PDP ditetapkan oleh Presiden dan bertanggung jawab kepada Presiden. Pengaturan kelembagaan lebih lanjut ditetapkan melalui Peraturan Presiden. [S6]

Pernyataan Komdigi pada 22 Juli menjelaskan pembentukan otoritas independen sedang difinalisasi. Pernyataan mengacu pada target periode penyelesaian. Tanggal yang diproyeksikan bukan bukti bahwa pembentukan telah selesai. [S10]

Keterangan Bawaslu pada 12 November mengutip ahli yang menyatakan lembaga pengawas belum dibentuk. Keterangan kegiatan ELSAM juga menjelaskan pejabat Komdigi membahas formalitas regulasi yang masih tertunda. Keduanya merupakan pernyataan bertanggal dengan jenis sumber berbeda. [S9][S56]

Laporan tidak menggantikan lembaga Pasal 58 dengan kementerian atau menyatakan penetapan yang tidak dibuktikan sumber pendukung. Organisasi perlu menyimpan kontak pelaporan resmi yang relevan dan memastikan saluran yang berlaku saat kewajiban timbul.

Ketidakpastian kelembagaan tidak boleh menghapus tanggung jawab internal. Pengendali tetap memerlukan penanggung jawab insiden, penilaian privasi, dan catatan pendukung tindakannya. Jalur pelaporan sektoral juga mungkin berlaku.

10.5 Pelaporan IIV memiliki jalur organisasi yang ditetapkan

Perpres 82/2022 menetapkan kerangka pelindungan infrastruktur informasi vital. Cakupannya meliputi identifikasi, pelindungan, pengawasan, dan koordinasi. BSSN menjadi koordinator, dengan kementerian dan regulator bertanggung jawab atas sektornya. [S11][S12][S13]

Pasal 13 mewajibkan tim tanggap insiden organisasi melaporkan insiden siber IIV kepada tim sektoral. Tim nasional menerima tembusan. Jangka waktunya paling lambat 1 × 24 jam setelah insiden ditemukan. [S12]

Jika tim sektoral terkait belum dibentuk, laporan ditujukan kepada kementerian atau lembaga yang bertanggung jawab, dengan tembusan kepada tim nasional. Jangka waktu yang sama berlaku. [S12]

Ini merupakan kewajiban IIV. Ini bukan tenggat universal bagi setiap situs usaha. Penanggung jawab hukum dan layanan organisasi perlu mengidentifikasi infrastruktur terdampak serta penetapan yang berlaku sebelum menggunakan peta pelaporan.

Tim respons perlu memelihara daftar kontak yang telah diuji. Rencana yang menyebut penerima tetapi tidak memiliki jalur pengiriman terkini menyisakan celah praktis. Latihan perlu mencakup tanda terima dan jalur alternatif.

10.6 Pelaporan siber bank umum tetap terpisah

SEOJK 29/SEOJK.03/2022 membahas ketahanan dan keamanan siber bagi bank umum konvensional dan bank umum syariah. Bagian IX menetapkan notifikasi awal dan laporan insiden siber yang lebih lengkap. [S14][S15]

Notifikasi awal disampaikan kepada OJK dalam 24 jam setelah bank mengetahui insiden siber. Notifikasi ditujukan secara tertulis dan elektronik kepada pengawas bank. Bank perlu memastikan OJK menerimanya. [S15]

Laporan lebih lengkap disampaikan melalui sistem pelaporan OJK dalam lima hari kerja setelah insiden siber diketahui. Ini merupakan hari kerja, bukan hari kalender. [S15]

Jika otoritas lain mensyaratkan notifikasi atau pelaporan lebih cepat, surat edaran mengatur penyampaian bersamaan kepada OJK dengan jangka waktu tersebut. Hal ini memerlukan penilaian keberlakuan, bukan satu asumsi untuk seluruh lembaga. [S15]

Catatan resmi OJK menyatakan bahwa PADK 1/2026 berlaku pada 1 Maret 2026 dan mencabut SEOJK 21/SEOJK.03/2017. [S16] Cakupan pelaporan terperincinya belum dipastikan secara independen dari teks asli. [S17]

Pembaruan kebijakan perlu mempertahankan pembedaan tersebut. Mengganti rujukan yang tidak berlaku lagi berguna. Namun, menyalin paragraf pelaporan non-siber ke rencana respons siber dapat menimbulkan kesalahan baru.

10.7 Pelaporan BI menggunakan jangka waktu awal yang lebih singkat

PADG 24/2024 melaksanakan kerangka keamanan informasi dan ketahanan siber BI. Cakupan yang dinyatakan mencakup penyelenggara sistem pembayaran, pelaku pasar uang dan pasar valuta asing, serta pihak lain yang diatur dan diawasi BI. [S18]

Pasal 45 mewajibkan notifikasi awal siber dalam satu jam setelah penyelenggara mengetahui insiden. Laporan insiden yang lebih lengkap harus disampaikan dalam tiga hari kalender setelah kejadian. [S18]

Kata pemicunya berbeda. Insiden dapat memiliki perkiraan waktu kejadian dan waktu penemuan yang lebih kemudian. Catatan perlu mempertahankan keduanya, bukan menggunakan penanda waktu pertama yang dimasukkan dalam catatan insiden.

PADG 29/2026 berlaku pada 25 September 2026. Perubahan tersebut memperkuat sanksi pelaporan dan memperjelas kewenangan BI atas infrastruktur informasi vital keuangan. Perubahan secara tegas merujuk jangka waktu satu jam dan tiga hari kalender. [S19][S20]

Denda pelaporan insidental yang diubah adalah Rp5 juta untuk keterlambatan atau ketiadaan laporan yang disebutkan. Keberadaan ketentuan tersebut tidak membuktikan pengenaan denda dalam kasus tertentu. [S20]

10.8 Catatan bersama dapat mendukung penghitungan waktu yang berbeda

Kerangka	Kondisi atau pemicu	Penerima	Jangka waktu
UU 27/2022, Pasal 46	Terjadi kegagalan pelindung-an data pribadi	Subjek data dan lembaga; pemberitahuan publik dalam keadaan tertentu	Pemberitahuan tertulis dalam 3 × 24 jam [S6]
Perpres 82/2022, Pasal 13	Penemuan insiden siber yang memengaruhi IIV	Tim sektoral, dengan tem-busan kepada tim nasional; kementerian atau lembaga pengganti jika berlaku	Paling lambat 1 × 24 jam setelah penemuan [S12]
SEOJK 29/2022, Bagian IX	Bank mengetahui insiden si-ber	Pengawas OJK	Pemberitahuan awal tertulis secara elektronik dalam 24 jam [S15]
SEOJK 29/2022, Bagian IX	Bank mengetahui insiden si-ber	Sistem pelaporan OJK	Laporan lebih lengkap dalam lima hari kerja [S15]
PADG 24/2024, Pasal 45	Penyelenggara mengetahui insiden siber	Bank Indonesia	Notifikasi awal dalam satu jam [S18]
PADG 24/2024, Pasal 45	Insiden siber terjadi	Bank Indonesia	Laporan insiden dalam tiga hari kalender [S18]

Tabel merupakan perbandingan operasional ketentuan yang dikutip. Tabel bukan penetapan bahwa setiap baris berlaku bagi setiap organisasi atau setiap insiden.

Penanggung jawab hukum dan kepatuhan perlu memelihara daftar keberlakuan untuk layanan yang diatur. Pemimpin penanganan insiden perlu memelihara catatan kejadian. Penggabungan fungsi tersebut mendukung keputusan tepat waktu tanpa menghapus perbedaan hukum.

10.9 Latih bukti yang diperlukan untuk notifikasi

Catatan insiden perlu membedakan fakta terkonfirmasi, perkiraan, dan hal yang belum dipastikan. Catatan perlu menyimpan sumber setiap pembaruan penting. Cakupan awal perlu tetap disebut awal.

Catatan juga perlu menyimpan waktu ketika organisasi mengetahui setiap fakta. Kesimpulan berikutnya mengenai waktu kejadian tidak boleh diam-diam menggantikan penanda waktu penemuan awal.

Latihan perlu menguji penyusunan, pengesahan, pengiriman, dan tanda terima. Penanggung jawab hukum perlu menentukan penerima. Penanggung jawab komunikasi perlu memastikan petunjuk pelanggan sesuai dengan cakupan saat ini.

Penyelesaian berarti organisasi dapat menunjukkan pengambil keputusan, fakta yang mendasari, dan cara memastikan pengiriman. Templat saja tidak membuktikan kesiapan.

TEMUAN UTAMA

01
Petakan setiap kewajiban ke cakupan hukum dan penerimanya

02
Pertahankan kejadian dan penemuan sebagai penanda waktu terpisah

03
Latih notifikasi dengan pengesahan dan bukti pengiriman

BAB 11

Prospek bersyarat

11

PERTANYAAN BAB INI

Pengamatan mendatang apa yang mendasari perubahan prioritas pertahanan Indonesia?

4

Skenario perencanaan dengan sinyal eskalasi yang jelas

11.1 Penilaian memiliki tingkat keyakinan yang ditetapkan 102
11.2 Skenario pertama: penawaran akses cocok dengan akun saat ini 102
11.3 Skenario kedua: materi identitas muncul dalam alur penipuan 103
11.4 Skenario ketiga: peringatan mendahului gangguan terukur 103
11.5 Skenario keempat: pencantuman terkait pemerasan memiliki bukti tambahan 103
11.6 Pengamatan yang akan mengubah laporan 104

BAB 11

Prospek bersyarat

RINGKASAN

Bukti mendukung perencanaan untuk akses yang diiklankan, penyalahgunaan identitas, gangguan layanan, dan tekanan kesinambungan terkait pemerasan. Bukti tidak mendukung probabilitas serangan nasional atau prakiraan kerugian yang tepat. Setiap skenario berikut menyatakan pemicu, alternatif, dan pengamatan yang akan mengubah penilaian. Tingkat keyakinan melekat pada hal-hal tersebut. Gunakan skenario untuk menyiapkan keputusan, lalu lakukan eskalasi hanya ketika bukti saat ini mendukung kondisi yang relevan.

11.1 Penilaian memiliki tingkat keyakinan yang ditetapkan

Terdapat keyakinan tinggi bahwa iklan yang disimpan dan pencantuman Ransompedia ada dalam populasi yang dinyatakan. Keyakinan itu menyangkut publikasi. Keyakinan tidak beralih ke keaslian setiap kumpulan data atau izin yang diiklankan. [S1][S2]

Dukungan lebih kuat terdapat pada fakta tertentu yang dilaporkan pengendali dan otoritas dalam berkas kasus eksternal. Perkiraan awal, dugaan penyelidikan, dan kesimpulan yang diperselisihkan tetap dibatasi sumbernya. [S35][S36][S40][S44]

Laporan vendor memberikan pengamatan kampanye yang didukung bukti dan penafsiran khusus penerbit. Buktinya tidak memberikan gambaran nasional lengkap. Tanggal aktivitas terdahulu atau tidak diketahui membatasi kesimpulan mengenai aktivitas dalam periode ini. [S21][S28][S29][S42][S43]

Asumsi perencanaan berikut tidak mengubah pengamatan tersebut menjadi prakiraan statistik. Asumsi menjelaskan keputusan yang perlu disiapkan dan fakta baru yang mendasari penggunaannya.

11.2 Skenario pertama: penawaran akses cocok dengan akun saat ini

Iklan akses menjadikan validasi akun saat ini sebagai tugas kesiapan yang masuk akal. Sinyal pentingnya adalah kecocokan kredibel dengan akun yang dikelola dan aktif, atau sesi tanpa izin. [S1]

Alternatifnya adalah iklan sudah lama, tidak akurat, diperantarai, atau tidak berkaitan dengan lingkup layanan organisasi saat ini. Label sektor yang serupa tidak dapat memastikan kemungkinan tersebut.

Jika bukti internal mengonfirmasi akses tanpa izin, penanggung jawab identitas dan layanan perlu menentukan cakupan izin serta membatasi sesi terkait. Pemimpin penanganan insiden perlu menentukan apakah terjadi akses yang lebih luas atau paparan informasi.

Eskalasi perlu diturunkan jika penanggung jawab membuktikan akun telah nonaktif, ditangani, atau tidak terkait. Penutupan perlu menyimpan bukti tersebut. Iklan dengan keyakinan rendah tidak boleh membuat organisasi berada dalam keadaan darurat tanpa akhir.

11.3 Skenario kedua: materi identitas muncul dalam alur penipuan

Korpus memuat permintaan dokumen identitas dan dugaan kumpulan data verifikasi identitas. Pengamatan tersebut mendukung pengujian pertahanan terhadap penggunaan ulang dan penyamaran identitas. Pengamatan tidak membuktikan alur penerimaan pelanggan tertentu telah disalahgunakan. [S1]

Eskalasi memerlukan sinyal internal yang relevan. Contohnya penggunaan identitas berulang, wakil tanpa kewenangan, atau kecocokan kredibel antara materi yang diduga dan hubungan pelanggan yang dikelola.

Alternatifnya adalah iklan menyangkut materi lama, salah atribusi, atau belum dipastikan keasliannya. Karena itu, penanggung jawab pencegahan penipuan perlu menyimpan bukti yang menghubungkan sinyal eksternal dengan kasus internal.

Tindakan pelindungan perlu sesuai dengan hubungan yang tervalidasi. Peringatan dukungan pelanggan, peninjauan pemohon, dan pembatasan transaksi memerlukan penanggung jawab serta uji penyelesaian berbeda.

11.4 Skenario ketiga: peringatan mendahului gangguan terukur

Pemberitahuan kesiapsiagaan pemerintah mendukung pemeriksaan kesiapan layanan publik yang relevan. Pemberitahuan tidak membuktikan bahwa setiap teknik yang diperingatkan akan terjadi atau pelaku yang disebut mampu menyebabkan dampak yang diklaim. [S48]

Eskalasi perlu mengikuti penurunan layanan terukur, perubahan tanpa izin, atau kejadian tervalidasi lainnya. Penanggung jawab layanan perlu mencatat fungsi terdampak dan periodenya.

Alternatifnya adalah tidak ada dampak yang sesuai, pembatasan untuk pelindungan, atau masalah operasional terpisah. Keterangan pemblokiran November dan layanan global menunjukkan pentingnya alternatif tersebut. [S47][S50]

Respons kesinambungan dapat berjalan sementara atribusi belum dipastikan. Komunikasi pelanggan perlu menjelaskan status layanan dan jalur pemulihan resmi. Catatan insiden kemudian perlu membedakan penyebab terkonfirmasi dari hipotesis sebelumnya.

11.5 Skenario keempat: pencantuman terkait pemerasan memiliki bukti tambahan

Populasi pencantuman Ransompedia mendasari kesiapan menghadapi pemerasan dan jalur peninjauan yang ditetapkan. Pencantuman saja tidak membuktikan enkripsi, pengambilan data keluar, atau permintaan tebusan yang diterima organisasi. [S2]

Eskalasi mengikuti telemetri pendukung, laporan insiden yang diautentikasi, atau kejadian lain yang didukung bukti. Pemimpin penanganan insiden perlu menentukan layanan dan data yang terlibat.

Alternatifnya adalah dugaan tanpa bukti tambahan, materi berulang, atau pencantuman dengan cakupan berbeda dari deskripsi penjual. Organisasi perlu menyimpan hasil peninjauannya, bukan menyatakan hasil hanya berdasarkan pencantuman.

Pekerjaan kesinambungan perlu mencakup ketergantungan identitas dan urutan pemulihan. Pekerjaan privasi perlu menilai dampak informasi secara terpisah. Layanan yang pulih tidak menutup pertanyaan cakupan data.

11.6 Pengamatan yang akan mengubah laporan

Pengamatan baru	Penilaian yang berubah	Bukti yang diperlukan
Sesi berhak istimewa tanpa izin yang terkonfirmasi	Dugaan akses menjadi insiden akses saat ini	Bukti akun, sesi, dan izin
Pemberitahuan akhir pengendali mengenai cakupan data	Perkiraan awal akun atau jenis data dapat diperbarui	Keterangan pengendali bertanggal dan hubungan kasus
Penetapan resmi atau instrumen pelaksana	Status pembentukan lembaga pada waktu tertentu dapat berubah	Instrumen resmi yang berlaku
Gangguan layanan terukur yang sesuai dengan klaim	Peringatan atau dugaan memperoleh bukti dampak	Kronologi layanan dan korelasi kejadian
Tanggal aktivitas kampanye baru yang andal	Kronologi yang tidak diketahui atau terdahulu dapat diperjelas	Tanggal aktivitas dari sumber primer
Hasil transaksi dengan bukti tambahan	Potensi penyalahgunaan dapat menjadi kejadian keuangan yang tervalidasi	Transaksi yang direkonsiliasi dan kasus pelanggan

Pengamatan ini perlu mengubah hal tertentu yang dibahasnya. Instrumen resmi pembentukan lembaga tidak memvalidasi dugaan pelanggaran keamanan yang tidak terkait. Kumpulan data terkonfirmasi tidak membuktikan setiap izin akses yang diiklankan.

TEMUAN UTAMA

01
Kaitkan tingkat keyakinan dengan hal tertentu

02
Siapkan keputusan skenario sebelum pemicunya terjadi

03
Tingkatkan atau turunkan eskalasi dengan bukti saat ini

BAB 12

Rencana tindakan dengan tanggung jawab yang jelas

12

PERTANYAAN BAB INI

Siapa bertanggung jawab atas 30, 60, dan 90 hari mendatang, dan bukti apa yang menunjukkan penyelesaian?

90

Hari untuk peningkatan bertahap, bukan penundaan ancaman aktif

12.1 Keputusan pertama adalah apakah risiko masih berlaku 106
12.2 Jalur tiga puluh hari: tetapkan tanggung jawab dan fakta saat ini 106
12.3 Jalur enam puluh hari: uji jalur respons 108
12.4 Jalur sembilan puluh hari: tunjukkan penyelesaian yang bertahan 109
12.5 Ukuran yang dapat diminta pimpinan 110
12.6 Tanggung jawab menurut peran 110
12.7 Cara Brandefense mendukung alur kerja 111

BAB 12

Rencana tindakan dengan tanggung jawab yang jelas

RINGKASAN

Rencana yang berguna menghubungkan sinyal teramati dengan penanggung jawab, pemicu, dan uji penutupan. Akses tanpa izin yang masih berlangsung memerlukan respons segera. Jalur 30, 60, dan 90 hari mengurutkan peningkatan kemampuan di sekitar kewajiban tersebut. Prioritasnya adalah validasi akun, pemulihan layanan, keutuhan transaksi, dan kesiapan notifikasi. Pimpinan perlu meminta bukti penyelesaian dari penanggung jawab dan menampilkan cakupan yang belum dipastikan. Mulai dari antrean validasi risiko aktif dan tetapkan sponsor eksekutif.

12.1 Keputusan pertama adalah apakah risiko masih berlaku

Jadwal berikut merupakan jangka perencanaan. Jadwal tidak mengizinkan penundaan ketika akses tanpa izin atau aktivitas berbahaya yang masih berlangsung telah dibuktikan.

Klaim eksternal perlu masuk ke antrean validasi dengan penanggung jawab. Penanggung jawab perlu mencatat hal yang diperiksa, hubungan layanan, dan bukti saat ini yang tersedia. Pemimpin penanganan insiden menentukan eskalasi berdasarkan catatan itu.

Perubahan yang mengganggu operasi perlu mengikuti risiko tervalidasi dan penilaian dampak layanan. Hal ini terutama penting untuk identitas yang berhubungan dengan pelanggan, administrasi bersama, dan alur keuangan.

12.2 Jalur tiga puluh hari: tetapkan tanggung jawab dan fakta saat ini

10–30 hari

Tinjau iklan akses yang relevan jika masuk akal cocok dengan layanan yang dikelola

PENANGGUNG JAWAB

Penanggung jawab identitas dan layanan

BUKTI PENYELESAIAN

Keadaan akun, izin, peninjauan sesi, dan keputusan penanganan tercatat

Petakan setiap layanan kritis ke ketergantungan aplikasi, identitas, dan pemasoknya	
PENANGGUNG JAWAB Penanggung jawab manajemen layanan	BUKTI PENYELESAIAN Daftar ketergantungan yang disetujui dengan penanggung jawab yang ditetapkan
Pastikan keberlakuan pelaporan untuk setiap layanan yang diatur	
PENANGGUNG JAWAB Penanggung jawab hukum dan kepatuhan	BUKTI PENYELESAIAN Daftar penerima, pemicu, dan tenggat yang terhubung dengan instrumen berlaku
Pertahankan cakupan data pelanggan ketika muncul dugaan atau pengungkapan yang kredibel	
PENANGGUNG JAWAB Penanggung jawab privasi dan pemilik data	BUKTI PENYELESAIAN Catatan cakupan sesuai jenis data dengan kategori terkonfirmasi, potensial, dan belum dipastikan
Tinjau akses jarak jauh berhak istimewa setelah bukti akses saat ini atau perubahan yang belum terjelaskan	
PENANGGUNG JAWAB Operasi identitas	BUKTI PENYELESAIAN Keputusan sesi, peninjauan kelompok berhak istimewa, dan catatan pembatasan sesuai cakupan
Validasi inventaris komponen arsip Windows dan terapkan pembaruan vendor yang didukung jika rentan; prioritas berasal dari aktivitas terdahulu CVE-2025-8088 [S22][S25]	
PENANGGUNG JAWAB Penanggung jawab pengelolaan endpoint	BUKTI PENYELESAIAN Tidak ada WinRAR hingga 7.12 dalam cakupan yang disepakati, kecuali pengecualian dengan penanggung jawab; 7.13 merupakan minimum perbaikan, bukan target versi terbaru [S22][S25]

Jalur pertama perlu menghilangkan ketidakjelasan mengenai pihak yang dapat memvalidasi dugaan. Kotak masuk keamanan tanpa penanggung jawab bisnis dapat menerima sinyal sementara keputusan dasarnya belum dibuat.

Penanggung jawab insiden perlu melacak waktu hingga penetapan tanggung jawab selain waktu hingga penutupan. Kasus yang belum selesai perlu menyatakan fakta atau akses yang masih kurang. Kasus tidak boleh ditutup hanya karena tidak ada pembaruan publik.

12.3 Jalur enam puluh hari: uji jalur respons

131–60 hari		
Latih pemulihan satu alur pelanggan atau operasional yang kritis	PENANGGUNG JAWAB Penanggung jawab kesinambungan dan layanan	BUKTI PENYELESAIAN Hasil pemulihan yang diamati, ketergantungan yang diuji, dan pengecualian yang belum selesai
Latih pelaporan PDP, IIV, OJK, atau BI bersamaan jika berlaku	PENANGGUNG JAWAB Penanggung jawab hukum dan pemimpin insiden	BUKTI PENYELESAIAN Waktu keputusan, draf yang disahkan, latihan pengiriman, dan tanda terima
Uji apakah penggunaan identitas tanpa izin dapat melewati persetujuan keuangan	PENANGGUNG JAWAB Penanggung jawab kejahatan keuangan dan aplikasi	BUKTI PENYELESAIAN Cakupan uji terdokumentasi, hasil jalur persetujuan, dan pengecualian yang diperbaiki
Tinjau akses administrasi konten untuk situs yang dikelola secara tersebar	PENANGGUNG JAWAB Penanggung jawab layanan web	BUKTI PENYELESAIAN Administrator yang ditetapkan, jalur penerapan tepercaya, dan pemeriksaan pemulihan
Uji pemeriksaan kewenangan pemohon dan wakil terhadap skenario penggunaan ulang identitas	PENANGGUNG JAWAB Penanggung jawab operasional antipenipuan	BUKTI PENYELESAIAN Kasus yang disetujui, hasil eskalasi, dan penanggung jawab pengecualian

Latihan pemulihan perlu mencapai hasil bisnis. Latihan tidak boleh berakhir ketika server menyala atau berkas cadangan terbuka. Penanggung jawab layanan perlu menunjukkan bahwa alur yang diuji berfungsi.

Latihan notifikasi juga perlu menguji serah terima nyata. Pemimpin penanganan insiden menyediakan fakta. Tim hukum menentukan keberlakuan. Tim komunikasi menyiapkan panduan pelanggan. Penerima yang berwenang dan jalur pengiriman harus diketahui.

12.4 Jalur sembilan puluh hari: tunjukkan penyelesaian yang bertahan

161–90 hari		
Periksa ulang perbaikan kontrol eksternal yang telah diselesaikan dalam produksi	PENANGGUNG JAWAB Penanggung jawab infrastruktur	BUKTI PENYELESAIAN Pengamatan saat ini dan catatan perubahan yang ditutup
Validasi akses pemasok setelah perubahan layanan atau kontrak yang penting	PENANGGUNG JAWAB Penanggung jawab risiko pemasok dan identitas	BUKTI PENYELESAIAN Izin saat ini, konfirmasi penanggung jawab, dan keputusan pengecualian
Tinjau ekspor data bervolume tinggi dan isi log sensitif	PENANGGUNG JAWAB Penanggung jawab data dan aplikasi	BUKTI PENYELESAIAN Peran ekspor yang disetujui, peninjauan pemantauan, dan pengecualian pencatatan log yang ditangani
Uji komunikasi gangguan yang diautentikasi dan dukungan pelanggan alternatif	PENANGGUNG JAWAB Penanggung jawab komunikasi dan operasional pelanggan	BUKTI PENYELESAIAN Hasil latihan, saluran resmi, dan catatan perbaikan
Tinjau dugaan berulang terhadap catatan insiden sebelumnya	PENANGGUNG JAWAB Penanggung jawab manajemen insiden	BUKTI PENYELESAIAN Kasus yang terhubung, pemeriksaan akun saat ini, dan status penutupan yang beralasan

Jalur terakhir perlu mengurangi ketidakjelasan berulang. Iklan yang muncul kembali perlu memicu perbandingan dengan kasus sebelumnya, diikuti pemeriksaan risiko saat ini. Iklan tidak otomatis menciptakan insiden baru atau mewarisi penutupan yang sudah tidak sesuai.

Pengecualian kontrol juga perlu mempertahankan dampak layanannya. Penyelesaian teknis lebih kuat ketika penanggung jawab dapat menjelaskan jalur akses atau alur kerja yang berubah serta cara memeriksa hasilnya.

12.5 Ukuran yang dapat diminta pimpinan

Ukuran	Target rencana	Sumber bukti
Tanggung jawab atas sinyal eksternal yang relevan	Setiap sinyal dalam antrean yang disepakati memiliki penanggung jawab	Daftar insiden
Validasi akun saat ini	Setiap dugaan akses yang dieskalasi memiliki keputusan penanganan akun dan sesi tercatat	Catatan kasus identitas
Cakupan ketergantungan layanan kritis	Setiap layanan yang dipilih untuk program memiliki penanggung jawab ketergantungan yang disetujui	Daftar layanan
Bukti pemulihan	Setiap alur kritis terpilih memiliki hasil latihan yang diamati	Catatan kesinambungan
Kesiapan notifikasi	Setiap jalur pelaporan yang berlaku telah dilatih atau memiliki pengecualian eksplisit	Catatan latihan hukum dan insiden
Disiplin cakupan data	Setiap kasus data pelanggan memisahkan cakupan terkonfirmasi, potensial, dan belum dipastikan	Catatan kasus privasi
Rekonsiliasi keuangan	Setiap kasus transaksi yang dieskalasi mempertahankan status dan hasil pelanggan	Catatan kejahatan keuangan

Ini merupakan target penyelesaian yang diusulkan, bukan pengukuran yang sudah dicapai organisasi Indonesia. Sponsor eksekutif perlu menyepakati populasi layanan dan meninjau pengecualian.

Pembahasan dewan yang berguna menanyakan alasan kasus belum selesai dan keputusan berikutnya. Pembahasan tidak boleh memberi penghargaan atas turunnya jumlah peringatan jika tanggung jawab atau kualitas bukti memburuk.

12.6 Tanggung jawab menurut peran

CISO bertanggung jawab atas koordinasi bukti keamanan dan eskalasi. Penanggung jawab layanan bertanggung jawab atas dampak bisnis dan penerimaan pemulihan. Keduanya tidak perlu menyimpulkan keputusan satu sama lain dari dasbor.

Penanggung jawab identitas memvalidasi akun, sesi, dan hak akses. Penanggung jawab privasi menilai dampak data. Tim kejahatan keuangan memvalidasi transaksi. Hukum dan kepatuhan menentukan kewajiban pelaporan yang berlaku.

Komunikasi dan operasional pelanggan perlu menerima fakta terkini yang sama. Pesannya dapat singkat sekaligus mempertahankan hal yang belum dipastikan. Perubahan cakupan perlu dicatat dan dicerminkan secara konsisten.

Sponsor eksekutif menyelesaikan konflik tanggung jawab dan mendanai pekerjaan yang diperlukan. Peran itu terutama penting ketika pemasok bersama, situs yang dikelola tersebar, atau beberapa kewajiban pelaporan melintasi batas organisasi.

12.7 Cara Brandefense mendukung alur kerja

Laporan menggunakan pengamatan unggahan Brandefense Blackhole, pencantuman terkait pemerasan Ransompedia, dan konteks organisasi terpilih yang dijelaskan dalam Lampiran A. Setiap jenis pengamatan mendukung keputusan validasi yang berbeda. [S1][S2][S4]

Intelijen eksternal berguna ketika mencapai penanggung jawab yang jelas dengan konteks yang sesuai. Intelijen perlu menghubungkan dugaan, layanan relevan, dan periode dengan bukti organisasi sendiri.

Brandefense menjelaskan kemampuan intelijen ancaman siber, pelindungan terhadap risiko digital, dan permukaan serangan. Untuk membahas kemampuan tersebut sesuai alur kerja dalam laporan ini, minta demo. [S82]

Organisasi tetap bertanggung jawab memvalidasi akses saat ini, menilai dampak, dan menentukan responsnya. Rencana tindakan memperjelas tanggung jawab tersebut dan memberi setiap penanggung jawab uji penyelesaian.

TEMUAN UTAMA

01
Tetapkan penanggung jawab untuk setiap sinyal yang relevan

02
Uji pemulihan dan pelaporan dengan serah terima nyata

03
Tutup pekerjaan dengan bukti kondisi layanan yang dihasilkan

LAMPIRAN

Lampiran

A–D

PERTANYAAN BAB INI

Apa populasi, batas bukti, dan catatan sumber di balik keputusan?

4

Lampiran untuk cakupan, bukti, sumber, dan istilah

Lampiran A. Cakupan dan batas bukti 113

Lampiran B. Daftar bukti yang disamarkan 116

Lampiran C. Catatan verifikasi sumber 118

Lampiran D. Glosarium 121

Lampiran A. Cakupan dan batas bukti

Negara-negara pembanding dipilih sebagai contoh semata-mata untuk memberikan konteks; pemilihan tersebut tidak menyiratkan peringkat atau penilaian politik.

A.1 Periode pengamatan

Periode menurut tanggal unggahan adalah 1 Januari hingga 22 November 2026. Periode terkini adalah 8 hingga 22 November. Pengamatan dihimpun sebelum hari batas pengamatan berakhir. Publikasi berikutnya pada hari itu berada di luar gambaran ini.

Angka pemerasan menggunakan tanggal pencantuman. Keterangan vendor dan resmi mempertahankan tanggal aktivitas, penemuan, notifikasi, dan publikasi secara terpisah. Kejadian terdahulu dapat memberi konteks pertahanan tanpa dihitung sebagai aktivitas 2026.

A.2 Populasi tetap terpisah

Populasi	Satuan	Batas utama
Metadata unggahan berlabel negara	Unggahan dengan label negara dalam periode laporan	Label tidak membuktikan penargetan atau insiden berbeda
Korpus unggahan yang disimpan	Publikasi yang disimpan dalam cakup-annya	Bukti terpilih tidak memperkirakan relevansi seluruh populasi
Pencantuman terkait pemerasan	Pencantuman Ransompedia menurut tanggal pencantuman	Klaim dapat mengulang organisasi dan tidak membuktikan penyusupan
Portofolio kandidat terpilih	Domain utama dalam portofolio yang dinyatakan	Pemilihan tidak memperkirakan prevalensi nasional
Pengamatan pasif	Catatan yang dinilai untuk setiap kondisi	Cakupan berbeda menurut kondisi; pengamatan yang tidak tersedia bukan nol
Keterkaitan kredensial atau perangkat	Satuan yang dinyatakan dalam hasil	Hubungan dan keabsahan saat ini perlu divalidasi
Catatan kartu pembayaran	Catatan dalam korpus unggahan yang disimpan	Bukan paparan nasional, pencurian, atau kerugian penipuan
Berkas kasus publik	Kasus dengan jenis bukti yang jelas	Berkas kasus dapat memuat beberapa dugaan atau tonggak

Populasi metadata berlabel negara dan korpus unggahan yang disimpan berbeda. Proporsi yang diamati dalam korpus tidak diterapkan pada seluruh populasi berlabel. Volume unggahan bukan tingkat serangan. [S1]

Pengamatan pasif mencakup 241 dari 250 domain kandidat terpilih; sembilan tidak tersedia. Status TLS menggunakan basis 241 domain. Pengamatan header menggunakan basis HTTP terpisah sebesar 154 domain. Indeks gabungan kondisi keamanan atau penilaian sektor tidak disajikan. [S3][S4]

Atlas menyediakan angka utama nasional 59/100 untuk portofolio terpilih berisi 250 domain. Hanya penilaian nasional tersebut yang disajikan. Tabel sektor anonim melaporkan jumlah paparan secara terpisah. Catatan lama, iklan penjualan terkini, dan pengamatan pasif mempertahankan makna waktu serta tugas validasi yang berbeda. [S4]

A.3 Istilah bukti

"Diiklankan", "diklaim", dan "ditawarkan" mempertahankan dugaan pelaku. "Dilaporkan polisi" mempertahankan keterangan penyelidikan. "Pengendali mengungkapkan" mempertahankan pernyataan pengendali. Tidak ada yang diam-diam ditingkatkan menjadi hasil yang terbukti secara independen.

Klaim dapat memuat materi asli sambil melebihkan akses saat ini. Pengungkapan publik dapat memuat jumlah sementara. Karena itu, tingkat keyakinan melekat pada hal tertentu yang dinilai.

"Belum dibuktikan" menggambarkan hal yang belum dipastikan. Istilah itu tidak menyatakan klaim palsu atau membuktikan tidak ada insiden. Laporan tidak menyimpulkan penjualan selesai atau pembayaran tebusan dari harga penawaran.

A.4 Hubungan dan penyamaran

Persona, unggahan, kumpulan data, label kelompok, dan organisasi merupakan konsep terpisah. Garis peta mengidentifikasi jenis buktinya. Alat bersama atau judul berulang tidak otomatis membuktikan operator yang sama.

Korban digambarkan menurut peran, kecuali keputusan penamaan memenuhi ketentuan publikasi. Kutipan publik menghapus materi pengenal atau kontak. Rujukan sumber asli tetap berada dalam catatan bukti privat.

Jika URL artikel dapat mengidentifikasi korban yang namanya tidak ditampilkan, Lampiran C menggunakan alamat utama penerbit atau tidak menampilkan URL. Hal ini mempertahankan perbedaan antara keterangan yang dapat dikutip dan izin mengungkap organisasi terdampak.

A.5 Batas yang memengaruhi keputusan

Portofolio terpilih bukan survei nasional. Korpus tidak membuktikan seluruh insiden siber Indonesia. Jumlah pencantuman tidak membuktikan kerugian, enkripsi, atau organisasi terdampak yang unik.

Hasil yang tidak berubah pada satu titik pengamatan tidak membuktikan kontrol beroperasi sepanjang tahun. Pengungkapan berikutnya tidak membuktikan awal aktivitas yang mendasarinya.

Perbandingan hukum menjelaskan ketentuan yang dikutip beserta cakupan dan waktunya. Keberlakuan bagi organisasi memerlukan penilaian layanan dan hukum saat ini. Target rencana tindakan merupakan kriteria penyelesaian yang diusulkan, bukan kinerja nasional yang diamati.

Lampiran B. Daftar bukti yang disamarkan

Berkas kasus	Bukti	Makna tanggal	Ditampilkan dalam
A–I	Iklan yang disimpan dan klaim peredaran	Tanggal unggahan yang diberikan; akses saat ini dan hasil tetap terpisah	Bab 4
J	Pengungkapan pengendali platform pelanggan dan tindak lanjut regulasi	Pengungkapan 28 Oktober; tindak lanjut 5 November	Bab 4
K	Keterangan polisi mengenai bank daerah dan pelaporan pengaduan awal	Aktivitas 22 Februari; tonggak penyelidikan berikutnya	Bab 4 dan 9
L	Keterangan penyelidikan pendanaan pendidikan	Transaksi Desember 2025 dan Januari 2026	Bab 4
M	Penyelidikan penjualan akses situs	Publikasi Juli dan pembaruan September	Bab 4 dan 5
N	Keterangan aplikasi kepegawaian yang diperselisihkan	Penemuan, notifikasi, dan pelaporan Juni	Bab 4
O	Keterangan situs layanan daerah	Penonaktifan dan pelaporan Agustus	Bab 4
P–R	Berkas kasus klaim tambahan yang disimpan	Tanggal unggahan yang diberikan	Bab 4

Kartu	Berkas kasus	Tanggal unggahan	Sarana	Alias	Bahasa	Ditampilkan dalam
B01	A	2026-10-17	Iklan forum	updap	Inggris	Bab 4
B02	B	2026-10-31	Iklan forum	marlanwg	Inggris	Bab 4
B03	C	2026-10-29	Iklan forum	CocoMel0n	Inggris	Bab 4
B04	D	2026-11-22	Iklan forum	AFKForever	Inggris	Bab 4
B05	E	2026-11-21	Iklan forum	SUB-ZER0	Inggris	Bab 4
B06	F	2026-03-04	Iklan forum	DrBisoun0urs	Inggris	Bab 4
B07	G	2026-01-05	Iklan forum	sellingood	Inggris	Bab 4
B08	H	2026-01-12	Iklan forum	Darmanboy24	Inggris	Bab 4
B09	I	2026-11-12	Iklan forum	updap	Inggris	Bab 4
B10	P	2026-05-05	Iklan forum	alwayschina	Inggris	Bab 4

Kartu	Berkas kasus	Tanggal ungga-han	Sarana	Alias	Bahasa	Ditampilkan da-lam
B11	Q	2026-05-14	Iklan forum	Kyyzo	Inggris	Bab 4
B12	R	2026-06-12	Iklan forum	Governer	Inggris	Bab 4

Daftar menghubungkan bukti dengan hal yang dinyatakan. Daftar bukan jumlah insiden. Beberapa unggahan dapat mendukung satu berkas peredaran, dan beberapa tanggal dapat menjelaskan satu kejadian dasar.

Lampiran C. Catatan verifikasi sumber

Nomor sumber yang tidak tercantum telah dipensiunkan selama peninjauan dan tidak dikutip.

S1: Brandefense Blackhole, pengamatan unggahan terkait Indonesia yang dibatasi cakupannya. Data sendiri; tidak ada URL publik untuk data mentah. Diverifikasi pada 22 November 2026.

S2: Ransompedia, pencantuman terkait pemerasan berlabel negara menurut tanggal pencantuman. Data sendiri; tidak ada URL publik untuk data mentah. Diverifikasi pada 22 November 2026.

S3: Pengamatan pasif domain terpilih dengan cakupan menurut kondisi. Data sendiri; tidak ada URL publik untuk data mentah. Diverifikasi pada 22 November 2026.

S4: Pengamatan paparan Brandefense Atlas dan portofolio kandidat terpilih, 250 domain utama, dibaca 22 November 2026. Data sendiri; tidak ada URL publik untuk data mentah. Diverifikasi pada 22 November 2026.

S5: BPK, catatan resmi UU 27/2022. Sumber. Diverifikasi pada 23 November 2026.

S6: UU 27/2022, teks undang-undang asli. Sumber. Diverifikasi pada 23 November 2026.

S7: BPOM, persiapan penerapan PDP, 15 September 2026. Sumber. Diverifikasi pada 22 November 2026.

S8: Pemerintah Gianyar, persiapan PP 33/2026, 16 September 2026. Sumber. Diverifikasi pada 23 November 2026.

S9: Bawaslu Makassar, keterangan kegiatan PP 33/2026 dan status lembaga, 12 November 2026. Sumber. Diverifikasi pada 22 November 2026.

S10: Komdigi, pernyataan pembentukan lembaga, 22 Juli 2026. Sumber. Diverifikasi pada 22 November 2026.

S11: BPK, catatan resmi Perpres 82/2022. Sumber. Diverifikasi pada 23 November 2026.

S12: Perpres 82/2022, teks IIV asli. Sumber. Diverifikasi pada 23 November 2026.

S13: Sekretariat Kabinet, penjelasan kerangka IIV, 15 Juni 2022. Sumber. Diverifikasi pada 22 November 2026.

S14: OJK, catatan resmi SEOJK 29/2022. Sumber. Diverifikasi pada 23 November 2026.

S15: SEOJK 29/2022, surat edaran ketahanan siber bank umum. Sumber. Diverifikasi pada 23 November 2026.

S16: OJK, catatan resmi PADK 1/2026. Sumber. Diverifikasi pada 23 November 2026.

S17: PADK 1/2026, peraturan TI bank umum. Sumber. Situs tidak tersedia pada 23 November 2026; bagian pendukung belum dipastikan secara independen.

S18: BI, kerangka ketahanan siber PADG 24/2024. Sumber. Diverifikasi pada 23 November 2026.

S19: BI, ringkasan resmi PADG 29/2026. Sumber. Diverifikasi pada 23 November 2026.

S20: PADG 29/2026, teks perubahan asli. Sumber. Diverifikasi pada 23 November 2026.

S21: Check Point Research, Amaranth-Dragon, 4 Februari 2026. Sumber. Diverifikasi pada 22 November 2026.

S22: CVE Program, catatan terbit CVE-2025-8088. Sumber. Diverifikasi pada 22 November 2026.

S24: NVD, halaman catatan CVE-2025-8088. Sumber. Diverifikasi pada 22 November 2026.

S25: WinRAR, imbauan rilis final 7.13. Sumber. Diverifikasi pada 22 November 2026.

S26: RARLAB, catatan perubahan versi 7.13. Sumber. Diverifikasi pada 22 November 2026.

S27: ESET, riset eksploitasi WinRAR, 11 Agustus 2025. Sumber. Diverifikasi pada 22 November 2026.

S28: Check Point Research, SilentDelivery dan hipotesis kerangka pemasok CopperDragon, 10 November 2026. Sumber. Diverifikasi pada 23 November 2026.

S29: Kaspersky, kampanye pajak Silver Fox, 30 April 2026. Sumber. Diverifikasi pada 23 November 2026.

S35: Kepolisian, penyelidikan pendanaan pendidikan, 3 April 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 22 November 2026.

S36: Kepolisian, tindak lanjut penyelidikan bank daerah, 15 Juli 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 22 November 2026.

S37: ANTARA, pengaduan bank daerah, 23 Februari 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 22 November 2026.

S38: Kepolisian, penyelidikan penjualan akses situs, 30 Juli 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 23 November 2026.

S39: BSSN, panduan respons historis perubahan tampilan situs tanpa izin, Juni 2023; salinan yang dihosting lembaga peradilan resmi. Sumber. Diverifikasi pada 22 November 2026.

S40: detik, keterangan aplikasi kepegawaian yang diperselisihkan, 27 Juni 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 22 November 2026.

S41: Bali Tribune, keterangan situs layanan daerah, 10 Agustus 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 22 November 2026.

S42: Proofpoint, BlueMoon / UNK_QuietRacket, 9 September 2026. Sumber. Diverifikasi pada 22 November 2026.

S43: Kaspersky, StrikeShark, 24 Juni 2026. Sumber. Diverifikasi pada 22 November 2026.

S44: Fore Coffee, pemberitahuan privasi platform pelanggan, 28 Oktober 2026. Sumber. Diverifikasi pada 23 November 2026.

S45: detik, pemeriksaan Komdigi atas laporan platform pelanggan, 5 November 2026. Sumber. Diverifikasi pada 22 November 2026.

S46: Komdigi, keterangan peredaran kembali data lama, 2 Oktober 2026. Sumber. Diverifikasi pada 22 November 2026.

S47: Komdigi, keterangan ketersediaan terkait pemblokiran, 8 November 2026. Sumber. Diverifikasi pada 22 November 2026.

S48: Komdigi, pemberitahuan kesiapsiagaan sistem publik, 10 November 2026. Sumber. Diverifikasi pada 22 November 2026.

S49: Komdigi, koordinasi ancaman agen AI, 10 November 2026. Sumber. Diverifikasi pada 22 November 2026.

S50: Kemenkes CSIRT, penyampaian ulang resmi imbauan gangguan layanan global BSSN, 13 November 2026. Sumber. Diverifikasi pada 23 November 2026.

S51: Kepolisian, pemeriksaan fakta rumor serangan global, 21 November 2026. Sumber. Diverifikasi pada 23 November 2026.

S52: OJK, lokakarya ketahanan keuangan digital, 30 April 2026. Sumber. Diverifikasi pada 23 November 2026.

S53: OJK, panduan ketahanan pendanaan digital, 11 November 2026. Sumber. Situs tidak tersedia pada 23 November 2026; bagian pendukung terakhir diverifikasi pada 22 November 2026.

S56: ELSAM, keterangan kegiatan pembentukan lembaga, 4 November 2026. Sumber. Diverifikasi pada 22 November 2026.

S57: Kepolisian, keterangan penegakan hukum alat phishing, 22 April 2026. Sumber. Diverifikasi pada 22 November 2026.

S66: Kepolisian, keterangan etik penggunaan teknologi, 18 November 2026. Sumber (URL artikel tidak ditampilkan). Diverifikasi pada 22 November 2026.

S81: DataReportal / Kepios, Digital 2026 Indonesia; acuan akhir 2025. Sumber. Diverifikasi pada 22 November 2026.

S82: Brandefense, halaman permintaan demo dan ringkasan kemampuan. Sumber. Diverifikasi pada 22 November 2026.

S83: OSS: NIB sebagai pengenal resmi usaha. Sumber. Diverifikasi pada 22 November 2026.

S84: Layanan pencatatan sipil Jakarta: KTP sebagai kartu identitas elektronik penduduk. Sumber. Diverifikasi pada 22 November 2026.

S85: MITRE ATT&CK, T1189 Kompromi melalui kunjungan situs. Sumber. Diverifikasi pada 22 November 2026.

S86: MITRE ATT&CK, T1566.001 Lampiran spearphishing. Sumber. Diverifikasi pada 22 November 2026.

S87: RFC Editor, RFC 7489, DMARC. Sumber. Diverifikasi pada 22 November 2026.

S88: RFC Editor, RFC 7208, SPF. Sumber. Diverifikasi pada 22 November 2026.

S89: RFC Editor, RFC 6376, DKIM signatures. Sumber. Diverifikasi pada 22 November 2026.

S90: RFC Editor, RFC 4033, DNSSEC introduction and requirements. Sumber. Diverifikasi pada 22 November 2026.

S91: RFC Editor, RFC 8446, TLS. Sumber. Diverifikasi pada 22 November 2026.

S92: RFC Editor, RFC 6797, HSTS. Sumber. Diverifikasi pada 22 November 2026.

S93: W3C, Content Security Policy Level 3, Draf Kerja, tujuan dan penyampaian kebijakan. Sumber. Diverifikasi pada 22 November 2026.

S94: RFC Editor, RFC 7034, HTTP Header Field X-Frame-Options. Sumber. Diverifikasi pada 22 November 2026.

S95: WHATWG, Fetch Standard, X-Content-Type-Options. Sumber. Diverifikasi pada 22 November 2026.

S96: BSSN, Lanskap Keamanan Siber Indonesia 2023, diterbitkan 2024; salinan yang dihosting CSIRT kementerian resmi. Sumber. Diverifikasi pada 23 November 2026.

S97: BSSN, Peraturan BSSN 5/2025 tentang Peta Jalan Pelindungan Infrastruktur Informasi Vital Sektor Administrasi Pemerintahan 2025-2029, 19 Februari 2025. Sumber. Diverifikasi pada 23 November 2026.

Lampiran D. Glosarium

Istilah	Makna dalam laporan ini
DMARC	Domain-based Message Authentication, Reporting, and Conformance: kebijakan email yang membantu membatasi pemalsuan domain. Kebijakan teramati tidak membuktikan penerapan pada setiap pesan. [S87]
SPF	Sender Policy Framework mengizinkan server mengirim email menggunakan suatu domain. Catatan yang diterbitkan tidak menunjukkan apakah setiap pesan lolos validasi. [S88]
DKIM	DomainKeys Identified Mail menggunakan tanda tangan digital untuk mengaitkan email dengan domain penanda tangan. Catatan yang tidak teramati tidak membuktikan ketiadaan penandatanganan. [S89]
DNSSEC	Domain Name System Security Extensions membantu mengautentikasi data DNS dan mendeteksi perubahan tanpa izin. Bukti delegasi teramati tidak membuktikan validasi setiap jawaban atau menyediakan enkripsi. [S90]
TLS	Transport Layer Security melindungi data dalam perjalanan dari penyadapan dan perubahan tanpa izin. Status sertifikat teramati tidak menilai keamanan setiap layanan. [S91]
HSTS	HTTP Strict Transport Security mengarahkan browser menggunakan koneksi aman ke suatu situs. Header teramati tidak membuktikan pelindungan pada setiap layanan atau permintaan. [S92]
CSP	Content Security Policy memungkinkan browser membatasi sumber daya yang boleh dimuat atau dijalankan halaman. Header teramati membuktikan keberadaan kebijakan pada respons tersebut, bukan efektivitas pembatasan atau pelindungan di setiap halaman. [S93]
Header pelindungan frame	Header yang membatasi apakah browser boleh menampilkan halaman di dalam frame halaman lain, seperti X-Frame-Options. Keberadaan header teramati tidak membuktikan pelindungan efektif terhadap clickjacking atau cakupan di setiap halaman. [S94]
Header pelindungan jenis konten	Header seperti X-Content-Type-Options, yang nilai nosniff-nya mengarahkan browser memblokir skrip atau gaya dengan jenis konten yang dinyatakan tidak sesuai. Keberadaan header tidak membuktikan nilai nosniff yang valid atau cakupan di setiap respons. [S95]
Akun	Hubungan identitas atau aktivitas masuk; tidak otomatis merupakan orang unik
Tanggal aktivitas	Saat sumber menyatakan tindakan terjadi
Iklan	Publikasi yang menawarkan atau mencari materi, akses, atau layanan

Istilah	Makna dalam laporan ini
Harga penawaran	Ketentuan yang dinyatakan penjual atau pembeli; bukan nilai transaksi selesai
Klaim	Pernyataan yang statusnya dipertahankan hingga bukti relevan mendukungnya
Pengendali	Peran yang bertanggung jawab menentukan pemrosesan data pribadi menurut kerangka PDP [S6]
Korpus	Populasi unggahan yang disimpan sebagaimana dijelaskan dalam Lampiran A
Tanggal penemuan	Saat organisasi atau sumber menyatakan kejadian diketahui
Berkas kasus	Analisis kasus terbatas yang dapat memuat beberapa publikasi atau tonggak
Catatan kejadian	Kejadian sistem atau bisnis yang dicatat; tidak otomatis merupakan pengguna atau akun
Pencantuman terkait pemerasan	Publikasi bertanggal yang mengaitkan label dengan dugaan sasaran [S2]
IIV	Infrastruktur informasi vital dalam kerangka Indonesia yang di-kutip [S12]
KTP	Kartu identitas elektronik penduduk, sebagaimana dijelaskan sumber resmi pencatatan sipil [S84]
NIB	Pengenal resmi usaha, sebagaimana dijelaskan layanan OSS [S83]
Waktu kejadian	Perkiraan waktu atau waktu yang terbukti ketika insiden terjadi
Persona	Identitas publikasi atau alias, tanpa klaim mengenai identitas hukumnya
Hak akses	Izin yang diduga atau dibuktikan untuk suatu akun
Tanggal publikasi	Saat unggahan, pemberitahuan, atau laporan muncul
Peredaran kembali	Publikasi berikutnya atas dugaan atau materi terdahulu
Sesi	Konteks akses yang diautentikasi dan keadaannya perlu ditinjau terpisah
Ketergantungan pemasok	Layanan atau izin yang menjadi sandaran organisasi
Validasi	Penilaian dengan penanggung jawab atas hal tertentu yang memengaruhi respons
Hari kerja	Satuan waktu dalam ketentuan laporan lebih lengkap OJK yang dikutip [S15]

Tentang laporan ini

Odin by Brandefense menyiapkan edisi riset publik ini dari pengamatan terbatas dan sumber yang telah dibaca sebagaimana dijelaskan di atas. Laporan mendukung keputusan pimpinan, keamanan, layanan, pencegahan penipuan, dan privasi.

Bukti publik mempertahankan ketidakpastian dan menghapus pengenal sensitif korban. Laporan tidak mengklaim penjualan selesai, akses saat ini yang terverifikasi, atau insiden terkonfirmasi hanya karena suatu publikasi mengiklankannya.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO