Penyedia “Bulletproof” hosting: Tindakan keras pada infrastruktur penjahat siber

Penjahat siber yang sukses mengandalkan infrastruktur yang aman, tidak terdeteksi, dan tangguh. Di balik setiap kejadian kompromi jaringan, pencurian kredensial, ransomware, atau pencurian dan penjualan data di forum terlarang, terdapat infrastruktur aman yang memungkinkan penjahat siber untuk beroperasi dan tetap tersembunyi.

Namun, bagi penjahat siber, tetap tidak terdeteksi dan sulit dilacak semakin menjadi tantangan. Kolaborasi global antara pemerintah, penegak hukum, dan sektor swasta membuat mereka semakin sulit untuk tetap anonim secara daring. Selain itu, sangat sedikit penjahat siber yang memiliki keterampilan dan keahlian yang dibutuhkan untuk mengelola dan memelihara sendiri infrastruktur yang aman. Karena itu, mereka mencari penyedia infrastruktur terlarang yang dapat memberikan layanan ini atas nama mereka, yang memungkinkan penjahat siber untuk fokus pada korban dan mendapatkan keuntungan.

‘Sebagai layanan Kejahatan siber’ mengacu pada pasar gelap yang telah berkembang untuk mendukung berbagai pelaku kejahatan siber. Pasar bawah tanah ini terdiri dari berbagai macam alat, layanan, dan informasi yang dapat dibeli dan terus bertambah dan berkembang yang membantu penjahat siber dalam mencari korban daring. Calon penjahat siber dapat membeli akses ke jaringan, membeli alat untuk membantu menghindari langkah-langkah keamanan, serta membeli malware untuk disebarkan dan mencuri informasi pribadi korban. Penyedia Bulletproof hosting (BPH) merupakan bagian dari ekosistem ini dan menawarkan infrastruktur yang aman bagi para penjahat siber. Yang terpenting, satu penyedia BPH dapat secara langsung memungkinkan ratusan penjahat siber untuk menargetkan korban di seluruh dunia.

Apa itu penyedia “Bulletproof” hosting ?

Secara sederhana, penyedia BPH menyewakan infrastruktur virtual dan/atau fisik kepada para penjahat siber untuk beroperasi. Penyedia BPH merupakan kelas khusus layanan infrastruktur internet yang memungkinkan pelaku kejahatan (termasuk penjahat siber) untuk menghosting konten terlarang dan menjalankan operasi di internet.

Istilah "antipeluru" adalah pemasaran murni. Pada kenyataannya, layanan ini sama rentannya terhadap gangguan seperti penyedia infrastruktur lainnya. Sebaliknya, penyedia BPH menolak untuk mematuhi penegakan hukum dan permintaan penghapusan konten lainnya serta mengabaikan keluhan penyalahgunaan dari para korban dan pemberitahuan permintaan pelanggan. Artinya, pelaku kejahatan siber dapat berkomunikasi, menjalankan forum dan situs web terlarang, menyebarkan malware dan kampanye phishing, serta mencuci uang tanpa takut operator akan menghentikan sewa mereka atas permintaan penegak hukum atau permintaan lainnya.

Penyedia BPH secara sadar berpartisipasi dalam ekosistem kejahatan siber dan memungkinkan terjadinya kejahatan siber yang bermotif keuangan. Insiden Keamanan Siber besar yang memengaruhi organisasi Australia dan pelanggan mereka terjadi sebagai akibat dari penjahat yang memanfaatkan penyedia BPH. Konsekuensi dari insiden ini mencakup serangan ransomware yang mengganggu, pemerasan data, dan pencurian informasi sensitif.

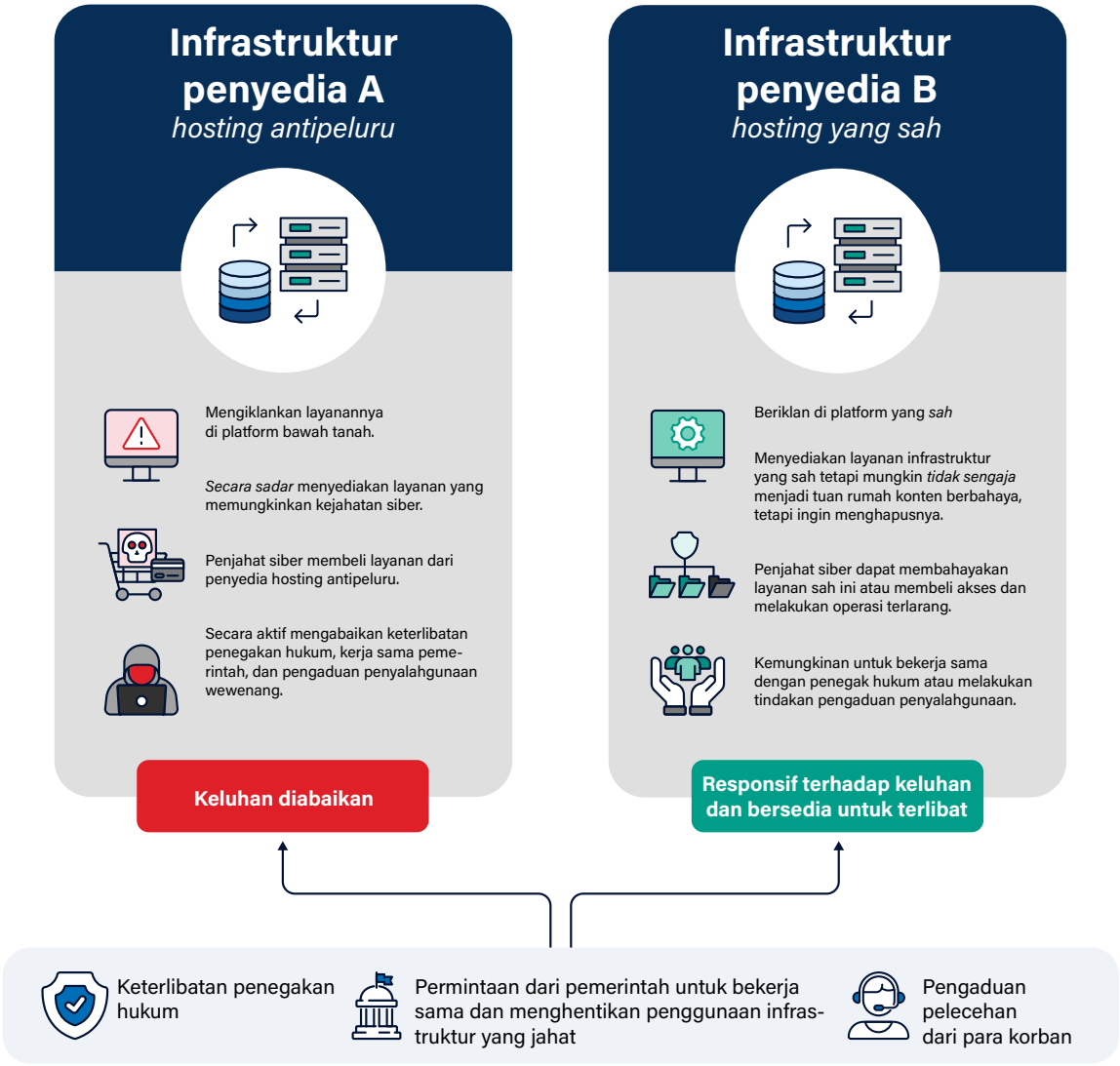
Representasi iklan penyedia hosting antipeluru di forum bawah tanah:

Bagaimana cara kerja penyedia BPH?

Model bisnis berbeda di antara penyedia BPH. Metode yang paling umum melibatkan penyewaan alamat IP kepada pelanggan penjahat siber dan menggunakan metode peralihan jaringan yang rumit untuk membantu mengaburkan lokasi, identitas, dan aktivitas mereka. Dalam banyak kasus, penyedia BPH menjual kembali atau menyewakan alamat IP dan server dari penyedia hosting, pusat data, atau Penyedia Layanan Internet (ISP) sah lainnya. Penyedia layanan ‘hulu’ ini mungkin tidak menyadari bahwa mereka menyediakan infrastruktur bagi penyedia layanan BPH yang kemudian menyediakan layanan ‘hilir’ bagi pelaku kejahatan siber.

Penyedia BPH mengonfigurasi jaringan dan arsitektur sistem mereka agar lebih sulit mengidentifikasi pelanggan mereka. Misalnya, mereka sering mengubah pengenal yang berhubungan dengan internet yang terkait dengan aktivitas pelanggan – seperti alamat IP dan nama domain yang ditetapkan. Metode yang paling umum melibatkan penyewaan alamat IP kepada pelanggan penjahat siber dan menggunakan metode peralihan jaringan yang rumit untuk membantu mengaburkan lokasi, identitas, dan aktivitas mereka. Selain itu, penyedia BPH sering menggunakan infrastruktur di negara-negara dengan rezim siber yang permisif, di mana langkah-langkah formal untuk menyelidiki dan mencegah aktivitas siber yang jahat tidak ada atau lunak.

Apa perbedaan penyedia hosting antipeluru dengan penyedia infrastruktur yang sah?



Bagaimana penyedia BPH penarget memengaruhi ancaman kejahatan siber

Penyedia BPH merupakan peluang berharga untuk mengganggu ratusan hingga ribuan penjahat siber sekaligus. Sejumlah penjahat siber dan pelaku siber jahat lainnya menggunakan layanan ini untuk mempermudah pelanggaran mereka – dengan percaya bahwa aktivitas mereka akan tetap tersembunyi dan operasional dalam menghadapi permintaan penghapusan atau pengaduan penyalahgunaan.

Namun, penegak hukum, lembaga Pemerintah, dan sektor swasta berkolaborasi untuk menargetkan dan mengganggu penyedia infrastruktur terlarang ini, termasuk melalui langkah-langkah Pertahanan seperti secara proaktif memblokir lalu lintas internet dari penyedia BPH yang dikenal. Kegiatan-kegiatan ini membantu mengurangi jumlah kejahatan siber yang berinteraksi dengan jaringan Australia dan jaringan sekutunya, dan mencakup penyedia infrastruktur dan ISP ‘hulu’ yang sah yang mungkin tanpa disadari memungkinkan penyedia BPH mengakses internet dan menyediakan infrastruktur yang aman bagi para pelaku kejahatan siber.

Penyedia BPH bukan satu-satunya kategori penyedia infrastruktur dalam ekosistem layanan kejahatan siber. Layanan ini melanggengkan dan memungkinkan ancaman kejahatan siber terhadap Australia dengan secara aktif mendukung kampanye kejahatan siber dan dengan sengaja menghalangi penyelidikan dan respons yang sah. Mengambil tindakan terhadap penyedia BPH menyoroti kerentanan layanan ini dan pelaku kejahatan siber yang menggunakannya.