Penyedia pengehosan “Kalis Peluru”: Retakan dalam perisai infrastruktur penjenayah siber

Penjenayah siber yang berjaya bergantung kepada infrastruktur yang teguh, tidak boleh dikesan dan berupaya untuk bertahan. Di sebalik setiap contoh pengkompromian jaringan, kredential yang dicuri, ransomware atau pencurian dan penjualan data dalam forum-forum haram, adalah infrastruktur teguh yang membolehkan penjenayah siber untuk beroperasi dan kekal tersembunyi.

Namun begitu, bagi penjenayah siber, untuk kekal tersembunyi dan sukar dikesan semakin menjadi satu cabaran. Kolaborasi global antara kerajaan, pihak penguatkuasa undang-undang, dan sektor awam semakin menyukarkan usaha mereka untuk kekal anonim dalam talian. Selain daripada itu, tidak ramai penjenayah siber yang memiliki kemahiran dan kepakaran yang diperlukan untuk mengurus dan menyelenggara infrastruktur yang teguh dengan sendiri. Oleh itu, mereka berusaha untuk mencari penyedia infrastruktur haram yang boleh menyampaikan perkhidmatan ini bagi mereka, justeru membenarkan penjenayah siber tersebut untuk berfokus atas mangsa dan keuntungan mereka.

‘Jenayah siber-sebagai-sebuah-perkhidmatan’ (‘Cybercrime-as-a-service’) merujuk kepada pasaran gelap yang telah berkembang untuk menyokong pelbagai pelaku siber yang berniat jahat. Pasaran gelap ini merangkumi peralatan, perkhidmatan, dan maklumat yang boleh dibeli yang senantiasa bertambah dan berubah bagi membantu penjenayah siber dalam memangsakan sasaran dalam talian mereka. Mereka yang ingin menjadi penjenayah siber boleh membeli akses kepada jaringan, membeli peralatan yang akan membantu mereka untuk mengelakkan langkah-langkah keselamatan, selain membeli malware yang akan diaturgerakkan ke atas para mangsa dan mencuri maklumat peribadi. Penyedia pengehosan kalis peluru (BPH) merupakan sebahagian daripada eko-sistem ini dan menawarkan infrastruktur yang teguh kepada penjenayah siber. Lebih penting lagi, satu penyedia BPH boleh membolehkan secara langsung beratus-ratus penjenayah siber untuk menyasarkan mangsa mereka di seluruh dunia.

Apakah yang dimaksudkan dengan penyedia pengehosan “Kalis Peluru”?

Ringkasnya, penyedia BPH menyewakan penjenayah siber sebuah infrastruktur maya dan/atau fizikal daripada mana mereka akan menjalankan operasi mereka. Penyedia BPH ialah satu kelas perkhidmatan infrastruktur internet khusus yang membenarkan pelaku-pelaku yang berniat jahat (termasuk penjenayah siber) untuk mengehoskan kandungan haram dan menjalankan operasi mereka dalam internet.

Frasa “kalis peluru” hanyalah buat tujuan pemasaran semata-mata. Secara realitinya, perkhidmatan-perkhidmatan ini tetap sama terdedah kepada penjejasan seperti para penyedia infrastruktur lain. Sebaliknya, penyedia BPH menolak untuk mematuhi penguatkuasaan undang-undang dan permintaan penurunan kandungan lain dan tidak peduli akan aduan penyalahgunaan daripada para mangsa dan notis permintaan para pelanggan. Ini bererti penjenayah siber boleh berkomunikasi, menjalankan forum-forum dan laman-laman web haram, mengaturgerakkan malware dan kempen pancingan, dan mengubah wang haram tanpa berasa takut bahawa pihak pengoperasi akan menamatkan sewaan mereka atas permintaan pihak penguatkuasa undang-undang atau permintaan pihak lain.

Penyedia BPH secara sedar menyertai eko-sistem jenayah siber dan membolehkan jenayah siber serius yang bermotivasikan keuntungan kewangan. Insiden-insiden keselamatan siber utama yang menjejaskan organisasi-organisasi Australia serta pelanggan mereka telah terjadi akibat pengumpilan (leveraging) yang dilakukan penjenayah terhadap penyedia BPH. Antara akibat insiden-insiden ini termasuklah serangan ransomware yang sangat mengganggu-gugat, peras ugut data dan pencurian maklumat sensitif.

Contoh iklan penyedia pengehosan kalis peluru dalam forum gelap:

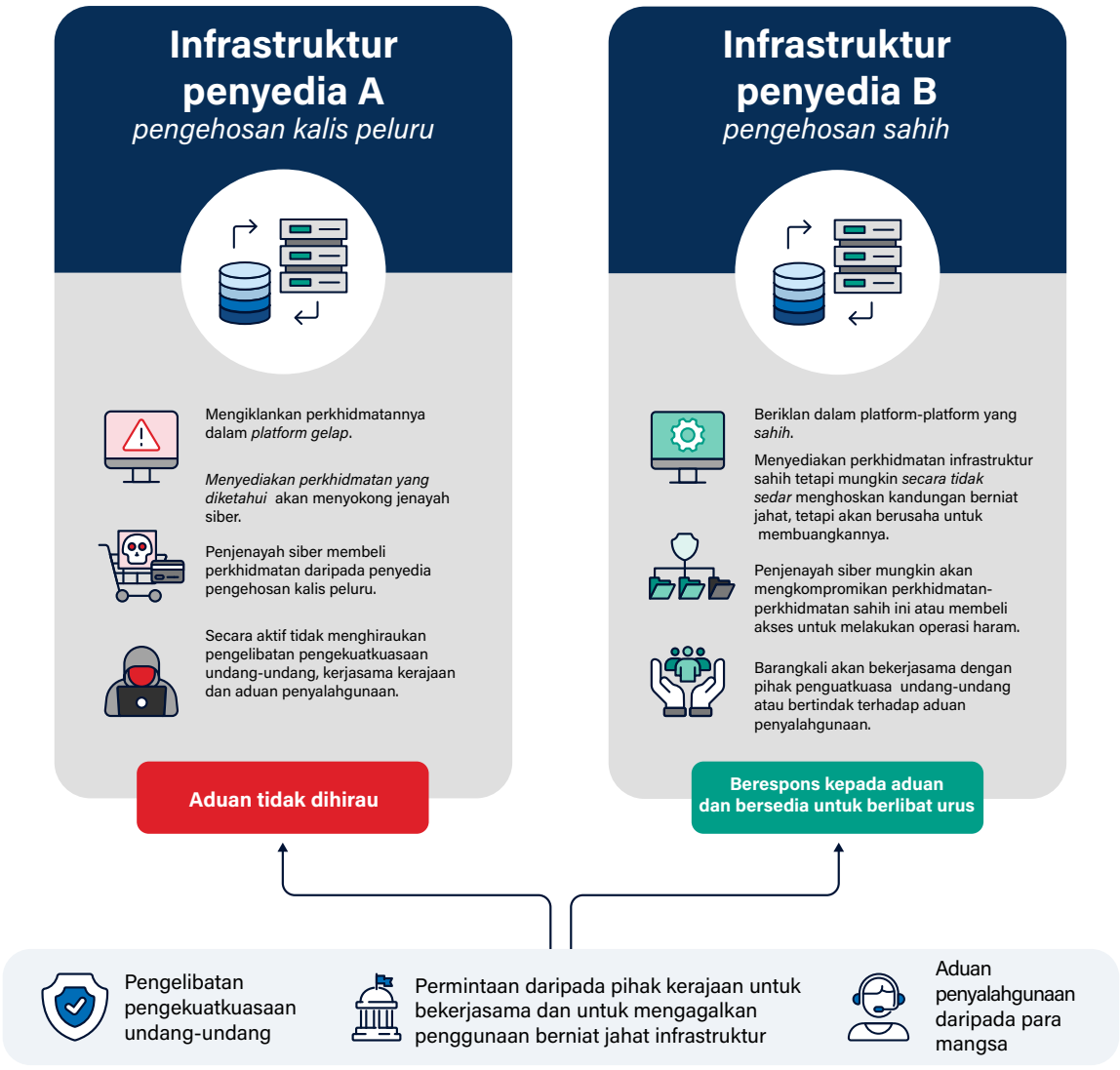
Bagaimana penyedia BPH melakukan kerja mereka?

Model-model perniagaan berbeza antara para penyedia BPH. Kaedah yang paling biasa mereka melibatkan penyewaan alamat-alamat IP kepada pelanggan penjenayah siber dan penggunaan kaedah pertukaran jaringan yang kompleks untuk membantu mengelabui lokasi, identiti dan kegiatan mereka. Dalam sebahagian besar kes, penyedia BPH menjual kembali atau menyewakan alamat-alamat dan server-server IP daripada penyedia pengehosan sahih, pusat-pusat data atau Penyedia Perkhidmatan Internet (Internet Service Providers) (ISPs) yang lain. Para penyedia “huluan” ini mungkin tidak sedar bahawa mereka sedang menyediakan infrastruktur kepada penyedia BPH yang kemudian menyediakan perkhidmatan “hiliran” kepada penjenayah siber.

Penyedia BPH mengkonfigurasikan jaringan dan arkitektur sistem mereka untuk menjadikannya lebih sukar untuk mengenalpasti pelanggan mereka. Contohnya, mereka sering menukar pengenalan identiti yang menghadap internet yang dikaitkan dengan kegiatan pelanggan mereka – misalnya alamat-alamat IP yang dikhususkan kepada mereka selain nama domain mereka. Teknik-teknik sebegini mencabar penahan dan

penyiasat dengan menjadikannya lebih sukar untuk mengaitkan sesebuah insiden dengan sesebuah alamat IP yang diguna seseorang pelaku atau pelanggan pada bila-bila masa. Tambahan pula, penyedia BPH sering menggunakan infrastruktur dalam negara-negara dengan regim-regim siber yang lebih longgar, di mana langkah-langkah formal untuk menyiasat dan menghalang kegiatan siber yang berniat jahat sama ada tidak-wujud sama sekali atau sangat longgar.

Bagaimanakah penyedia pengehosan kalis peluru berbeza daripada penyedia infrastruktur yang sahih



Bagaimana penyasaran penyedia BPH meninggalkan kesan terhadap ancaman jenayah siber

Penyedia BPH mewakili sebuah peluang berharga untuk mengganggu dan mematahkan ratusan hingga ribuan penjenayah siber dengan sekali gus. Pelbagai penjenayah siber dan para pelaku siber berniat jahat lain menggunakan perkhidmatan-perkhidmatan ini untuk memudahkan kegiatan jenayah mereka – atas keyakinan bahawa kegiatan mereka akan kekal dikelabui dan tetap beroperasi bila berhadapan dengan permintaan untuk menurunkan mereka atau aduan-aduan penyalahgunaan.

Namun begitu, pihak penguatkuasa undang-undang, agensi-agensi Kerajaan, dan sektor awam sedang berkolaborasi untuk menyasar dan mematahkan para penyedia infrastruktur haram ini, termasuk menerusi langkah-langkah Pertahanan seperti menghalang trafik internet secara proaktif daripada penyedia BPH yang dikenali. Kegiatan-kegiatan ini membantu mengurangkan jumlah bilangan jenayah siber daripada berinteraksi dengan jaringan-jaringan Australia dan sekutunya, dan termasuk penyedia infrastruktur dan ISPs “huluan” sahih yang mungkin tidak mengetahui bahawa mereka sedang membenarkan penyedia BPH untuk mengakses internet dan menyediakan infrastruktur teguh kepada penjenayah siber.

Penyedia BPH bukan satu-satunya kategori penyedia infrastruktur sahaja dalam eko-sistem jenayah siber-sebagai-satu-perkhidmatan. Perkhidmatan-perkhidmatan ini melangsungkan dan membenarkan ancaman jenayah siber ke atas Australia dengan menyokong secara aktif kempen-kempen jenayah siber dan dengan sengaja menghalang siasatan dan respons yang sah di sisi undang-undang. Pengambilan tindakan terhadap penyedia BPH menonjolkan kerentanan perkhidmatan-perkhidmatan ini serta pelaku siber berniat jahat yang menggunakannya.