Fornecedores de hospedagem “à prova de bala”: Fendas na armadura da infraestrutura cibercriminosa

Os cibercriminosos bem-sucedidos confiam em infraestruturas seguras, indetectáveis e resilientes Por detrás de cada caso de comprometimento da rede, de credenciais roubadas, de ransomware ou de roubo e venda de dados em fóruns ilícitos, há uma infraestrutura segura que permite que os cibercriminosos operem e permaneçam ocultos.

Porém, para os cibercriminosos, permanecer indetectáveis e difíceis de localizar está a tornar-se num desafio cada vez maior. A colaboração global entre os governos, as autoridades policiais e o sector privado está a tornar mais difícil o anonimato online. Além disso, muito poucos cibercriminosos têm as competências e os conhecimentos necessários para gerir e manter uma infraestrutura segura por si próprios. Como tal, procuram fornecedores de infraestruturas ilícitas que possam prestar este serviço em seu nome, permitindo que o cibercriminoso se concentre nas vítimas e no lucro.

O termo “cibercrime como serviço” refere-se ao mercado clandestino que se desenvolveu para apoiar uma série de ciberagentes maliciosos. Este mercado clandestino inclui uma gama cada vez maior e em evolução de ferramentas, serviços e informações adquiríveis que ajudam os cibercriminosos a vitimar alvos online. Os potenciais cibercriminosos podem comprar acesso a redes, adquirir ferramentas para ajudar a contornar as medidas de segurança, bem como comprar malware para utilizar contra as vítimas e roubar informações pessoais. Os fornecedores de hospedagem à prova de bala (BPH) fazem parte deste ecossistema e permitem infraestruturas seguras aos cibercriminosos. Mais importante, um fornecedor de BPH pode permitir diretamente que centenas de cibercriminosos atinjam vítimas em todo o mundo.

O que é um fornecedor de hospedagem “à prova de bala”?

Em termos simples, os fornecedores de BPH alugam aos cibercriminosos uma infraestrutura virtual e/ou física a partir da qual podem operar. Os fornecedores de BPH são uma classe específica de serviços de infraestruturas da Internet que permitem aos agentes maliciosos (incluindo os cibercriminosos) alojar conteúdos ilícitos e executar operações na Internet.

O termo “à prova de bala” é puro marketing. Na realidade, estes serviços são tão susceptíveis de sofrerem perturbações como os outros fornecedores de infraestruturas. Em vez disso, os fornecedores de BPH recusam-se a cumprir os pedidos das autoridades policiais e outros pedidos de remoção de conteúdos e ignoram as queixas de abuso das vítimas e os avisos de pedidos dos assinantes. Isto significa que os cibercriminosos podem comunicar, gerir fóruns e sítios Web ilícitos, lançar campanhas de malware e de phishing e fazer lavagem de dinheiro sem receio de que o operador rescinda o contrato de aluguer a pedido das autoridades policiais ou outras.

Os fornecedores de BPH participam conscientemente no ecossistema da cibercriminalidade e permitem uma cibercriminalidade grave com motivações financeiras. Os principais incidentes de cibersegurança que afectaram as organizações australianas e os seus clientes ocorreram em resultado de criminosos que tiraram partido dos fornecedores de BPH. As consequências destes incidentes incluíram ataques disruptivos de ransomware, extorsão de dados e roubo de informações sensíveis.

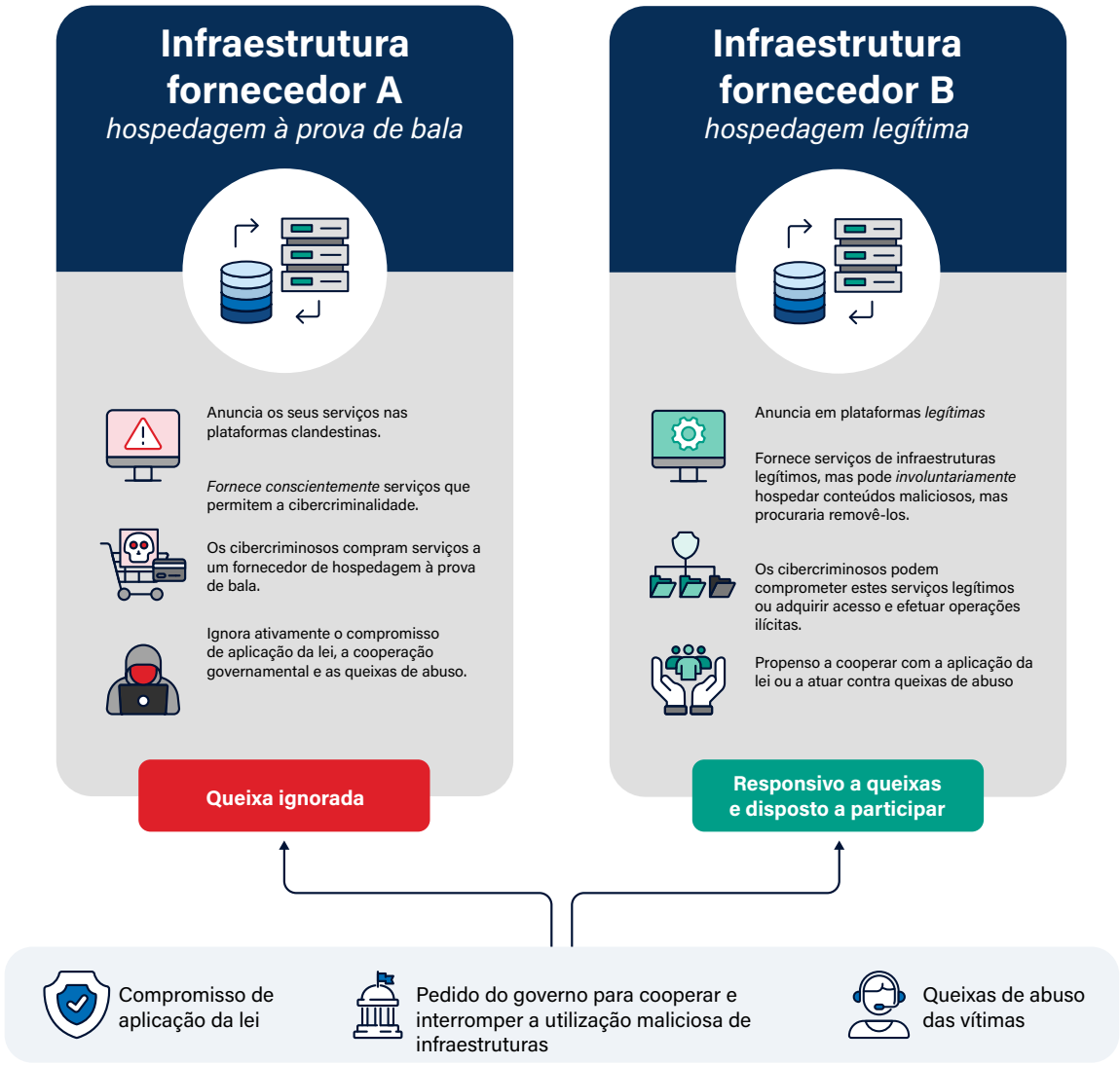
Representação de um anúncio de um fornecedor de hospedagem à prova de bala em fóruns clandestinos:

Como funcionam os prestadores de serviços de BPH?

O modelo de negócio difere entre os fornecedores de BPH. O método mais comum envolve o aluguer de endereços IP a clientes cibercriminosos e a utilização de métodos complexos de comutação de redes para ajudar a ocultar as suas localizações, identidades e atividades. Em muitos casos, os fornecedores de BPH revendem ou alugam endereços IP e servidores a outros fornecedores legítimos de hospedagem, centros de dados ou fornecedores de serviços Internet (ISPs). Estes fornecedores “a montante” podem não saber que estão a fornecer infraestruturas a fornecedores de BPH que, por sua vez, fornecem serviços “a jusante” aos cibercriminosos.

Os fornecedores de BPH configuram as suas redes e a arquitetura do sistema para dificultar a identificação dos seus clientes. Por exemplo, eles alteram frequentemente os identificadores de acesso à Internet associados à atividade do cliente, tais como os endereços IP e o nome de domínio que lhes foram atribuídos. Estas técnicas são um desafio para os defensores e investigadores porque dificultam a ligação entre um incidente e um endereço IP utilizado por um agente ou cliente num determinado momento. Além disso, os fornecedores de BPH utilizam frequentemente infraestruturas em países com regimes cibernéticos permissivos, onde as medidas formais para investigar e prevenir actividades cibernéticas maliciosas são inexistentes ou brandas.

Em que é que os fornecedores de hospedagem à prova de bala são diferentes dos fornecedores de infraestruturas legítimos?



Como é que o facto de almejar os fornecedores de BPH afecta a ameaça da cibercriminalidade

Os fornecedores de BPH representam uma oportunidade valiosa para perturbar centenas a milhares de cibercriminosos de uma só vez. Uma série de cibercriminosos e outros agentes cibernéticos maliciosos utilizam estes serviços para facilitar os seus crimes, confiantes de que a sua atividade permanecerá ofuscada e operacional face a pedidos de remoção ou queixas de abuso.

No entanto, as forças policiais, as agências governamentais e o sector privado estão a colaborar no sentido de visar e desmantelar estes fornecedores de infraestruturas ilícitas, incluindo através de medidas Defensivas, como o bloqueio proactivo do tráfego de internet de fornecedores de BPH conhecidos. Estas actividades ajudam a reduzir a quantidade de cibercrime que interage com as redes australianas e aliadas, e incluem fornecedores de infraestruturas e ISPs legítimos “a montante” que, sem saber, podem estar a permitir que os fornecedores de BPH acedam à Internet e forneçam infraestruturas seguras aos cibercriminosos.

Os fornecedores de BPH não são a única categoria de fornecedores de infraestruturas no ecossistema do cibercrime como serviço. Estes serviços perpetuam e permitem a ameaça da cibercriminalidade na Austrália, apoiando ativamente as campanhas de cibercriminalidade e impedindo deliberadamente a investigação e a resposta legais. A tomada de medidas contra os fornecedores de BPH realça a vulnerabilidade destes serviços e dos ciberagentes maliciosos que os utilizam.