"बुलेटप्रूफ" होस्टिंग प्रोवाइडर्स: साइबरक्रिमिनल ढांचे के कवच में दरारें

सफल साइबर-अपराधी एक सुरक्षित, छिपे हुए और लचीले ढांचे पर निर्भर करते हैं। नेटवर्क में घुसपैठ, चोरी की गई पहचानों, रैंसमवेयर, या डेटा की चोरी और अवैध फोरमों पर बिक्री के हरेक उदाहरण के नीचे एक सुरक्षित ढांचा होता है, जो साइबर-अपराधियों को अपना काम करने और छिपे रहने में सक्षम बनाता है।

लेकिन साइबर-अपराधियों के लिए छिपे रहना और और पीछा करने में कठिन होना एक बड़ी चुनौती बनता जा रहा है। सरकारों, कानून प्रवर्तन और निजी क्षेत्र के बीच वैश्विक सहयोग से उनके लिए ऑनलाइन गुमनाम बने रहना कठिन हो रहा है। इसके अलावा बहुत कम साइबर-अपराधियों के पास आवश्यक कुशलताएं और विशेषज्ञता होती है, ताकि वे अपने दम पर सुरक्षित ढांचे का प्रबंध कर सकें और इसे बरकरार रख सकें। इस कारण से साइबर-अपराधी ऐसे अवैध ढांचा प्रोवाइडर्स की खोज करते हैं जो उनकी ओर से यह सेवा उपलब्ध करा सकें, ताकि वे अपने शिकार लोगों पर ध्यान केंद्रित करने में सक्षम बन सकें और फायदा उठा सकें।

'साइबरक्राइम-एज़-ए-सर्विस' से संदर्भ ऐसे छिपे हुए बाज़ार से है, जो अनेकानेक दुर्भावनापूर्ण साइबरकर्मियों के समर्थन के लिए विकसित हुआ है। इस छिपे हुए बाज़ार में खरीदे जा सकने वाले टूल्स, सेवाओं और सूचनाओं की एक बढ़ती और विकसित होती हुई श्रृंखला शामिल है, जो ऑनलाइन लक्ष्यों को शिकार बनाने में साइबर-अपराधियों को सहायता देती है। भविष्य के साइबर-अपराधी नेटवर्कों के लिए एक्सेस, सुरक्षात्मक उपायों से बचने में सहायता के लिए टूल्स, और साथ ही ऐसे मैलवेयर भी खरीद सकते हैं, जिसका उपयोग उनके शिकार लोगों के प्रति किया जा सकता है और व्यक्तिगत जानकारी की चोरी की जा सकती है। बुलेटप्रूफ होस्टिंग (बीपीएच) प्रोवाइडर्स इस पारिस्थितिकी-तंत्र का एक हिस्सा होते हैं और वे साइबर-अपराधियों को सुरक्षित ढाँचा उपलब्ध कराते हैं। महत्वपूर्ण रूप से, मात्र एक ही बीपीएच प्रोवाइडर पूरी दुनिया-भर में शिकार लोगों को लक्षित करने के लिए सैकड़ों साइबर-अपराधियों को सीधे सक्षम बना सकता है।

"बुलेटप्रूफ" होस्टिंग प्रोवाइडर क्या है?

सादे शब्दों में कहें, तो बीपीएच प्रोवाइडर्स साइबर-अपराधियों को उनके काम के लिए एक वर्चुअल और/या वास्तविक ढांचा लीज़ पर देते हैं। बीपीएच प्रोवाइडर्स इंटरनेट ढांचा सेवा का एक विशिष्ट वर्ग होते हैं, जो दुर्भावनापूर्ण कर्मियों को (जिसमें साइबर-अपराधी भी शामिल हैं) अवैध सामग्री को होस्ट करने और इंटरनेट पर अपना काम करने में सक्षम बनाते हैं।

"बुलेटप्रूफ" शब्द केवल मार्केटिंग के लिए ही है। वास्तव में, अन्य ढांचा प्रोवाइडर्स के समान ही ये सेवाएं भी रोकथाम के प्रति अतिसंवेदनशील होती हैं। इसके बजाय, बीपीएच प्रोवाइडर्स कानून प्रवर्तन और सामग्री टेकडाउन के अन्य निवेदनों का अनुपालन नहीं करते हैं और शिकार लोगों की ओर से शोषण की शिकायतों और सब्सक्राइबर रिक्वेस्ट सूचनाओं को अनदेखा करते हैं। इसका अर्थ है कि साइबर-अपराधी संचार कर सकते हैं, अवैध फोरम्स और वेबसाइटें चला सकते हैं, मैलवेयर और फिशिंग के तरीके लागू कर सकते हैं, और इस डर के बिना मनी लॉन्डरिंग कर सकते हैं कि ऑपरेटर कानून प्रवर्तन की ओर से या अन्य निवेदनों पर अपनी लीज़ समाप्त कर देगा।

बीपीएच प्रोवाइडर्स जानबूझकर साइबर-अपराध पारिस्थितिकी-तंत्र में शामिल होते हैं और पैसों से प्रेरित गंभीर साइबर अपराध को सक्षम बनाते हैं। बीपीएच प्रोवाइडर्स का लाभ उठाने वाले अपराधियों के कारण ऑस्ट्रेलियाई संगठनों और उनके ग्राहकों को प्रभावित करने वाली कई प्रमुख साइबर सुरक्षा घटनाएं हुई हैं। इन घटनाओं के परिणामों में रैंसमवेयर के घुसपैठ हमले, जबरन डेटा वसूली और संवेदनशील जानकारी की चोरी शामिल है।

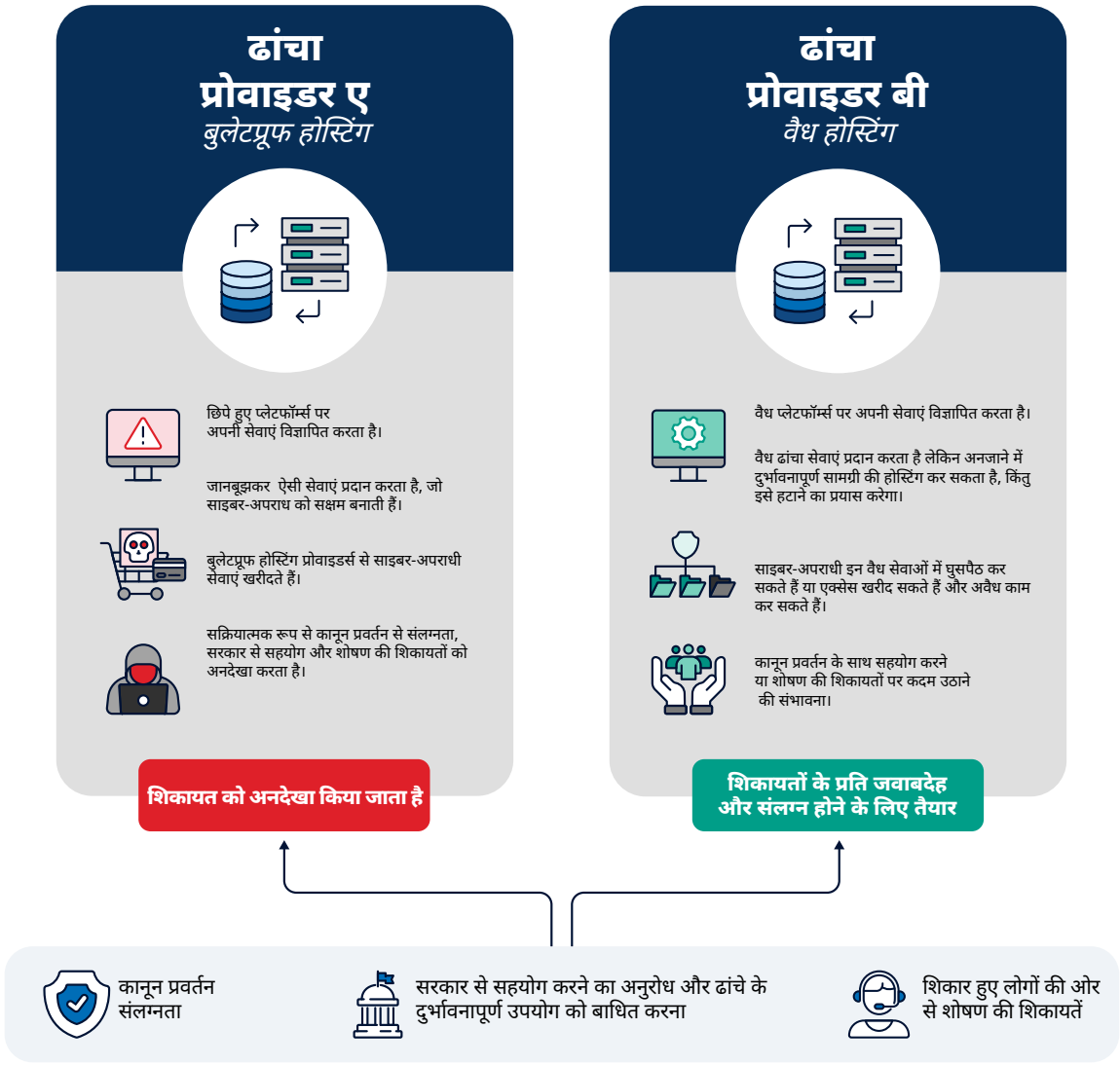
छिपे हुए फोरम्स में बुलेटप्रूफ होस्टिंग प्रोवाइडर्स का एक प्रतिनिधि विज्ञापन:

बीपीएच प्रोवाइडर्स कैसे काम करते हैं?

बीपीएच प्रोवाइडर्स के बीच व्यापार मॉडल अलग-अलग होता है। सबसे सामान्य विधि में साइबरक्रिमिनल ग्राहकों को लीज़ पर आईपी एड्रेसेज़ देना और उनके स्थानों, पहचानों और गतिविधियों को अस्पष्ट बनाने में सहायता के लिए जटिल नेटवर्क स्विचिंग विधियों का उपयोग करना शामिल है। कई मामलों में, बीपीएच प्रोवाइडर्स अन्य वैध होस्टिंग प्रोवाइडर्स, डेटा सेंटर्स या इंटरनेट सर्विस प्रोवाइडर्स (आईएसपी) से प्राप्त हुए आईपी एड्रेसेज़ और सर्वर्स को फिर से बेचते हैं या लीज़ पर देते हैं। ये 'अपस्ट्रीम' प्रोवाइडर्स इस बात से अनजान हो सकते हैं कि वे बीपीएच प्रोवाइडर्स को एक ढांचा प्रदान कर रहे हैं, जो साइबर-अपराधियों को 'डाउनस्ट्रीम' सेवाएं प्रदान करते हैं।

बीपीएच प्रोवाइडर्स अपने ग्राहकों की पहचान कठिन बनाने के लिए अपने नेटवर्क और सिस्टम आर्किटेक्चर का कॉन्फ़िग्युरेशन करते हैं। उदाहरण के लिए, वे ग्राहक की गतिविधि से जुड़े इंटरनेट पर प्रदर्शित होने वाले आइडेंटिफायर्स को अक्सर बदलते रहते हैं - जैसे उन्हें असाइन किए गए आईपी एड्रेसेज़ और डोमेन नेम्स। इस तरह की तकनीकें रक्षकों और जांचकर्ताओं के लिए चुनौती होती हैं, जिससे किसी घटना के समय किसी अपराधी या ग्राहक द्वारा उपयोग किए जा रहे आईपी एड्रेस के साथ उस घटना को जोड़ना कठिन हो जाता है। इसके अलावा, बीपीएच प्रोवाइडर्स अक्सर ढीली-ढाली साइबर व्यवस्थाओं वाले देशों में स्थित ढांचे का उपयोग करते हैं, जहां दुर्भावनापूर्ण साइबर-गतिविधि की जांच और रोकथाम के लिए औपचारिक नियम या तो मौजूद ही नहीं हैं या फिर बहुत सख्त नहीं हैं।

बुलेटप्रूफ होस्टिंग प्रोवाइडर्स वैध ढांचा प्रोवाइडर्स से अलग कैसे हैं?



बीपीएच प्रोवाइडर्स को लक्षित करने से साइबर-अपराध के खतरे पर क्या प्रभाव पड़ता है

बीपीएच प्रोवाइडर्स एक मूल्यवान अवसर का प्रतिनिधित्व करते हैं, जिससे एक ही बार में सैकड़ों से लेकर हजारों साइबर-अपराधी बाधित किए जा सकते हैं। अनेकानेक साइबर-अपराधी और अन्य दुर्भावनापूर्ण साइबरकर्मी अपने कृत्यों को आसान बनाने के लिए इन सेवाओं का उपयोग करते हैं – वे ऐसा मानते हैं कि टेकडाउन के निवेदन या शोषण की शिकायतें किए जाने पर उनकी गतिविधि अस्पष्ट और चालू बनी रहेगी।

लेकिन कानून प्रवर्तन, सरकारी एजेंसियां और निजी क्षेत्र इन अवैध ढांचा प्रोवाइडर्स को लक्षित और बाधित करने के लिए सहयोग कर रहे हैं, जिसमें रक्षात्मक उपायों के माध्यम से ऐसा किया जाना शामिल है, उदाहरण के लिए ज्ञात बीपीएच प्रोवाइडर्स से इंटरनेट ट्रैफ़िक को सक्रियात्मक तरीके से ब्लॉक करना। ये गतिविधियाँ ऑस्ट्रेलियाई और संबद्ध नेटवर्कों के साथ व्यवहार करने वाले साइबर-अपराधों को घटाने में मदद करती हैं और इसमें ऐसे वैध 'अपस्ट्रीम' ढांचा प्रोवाइडर्स और आईएसपी शामिल हैं, जो अनजाने में ही बीपीएच प्रोवाइडर्स को इंटरनेट एक्सेस करने में सक्षम बना सकते हैं और साइबर-अपराधियों को सुरक्षित ढांचा उपलब्ध करा सकते हैं।

साइबरक्राइम-एज़-ए-सर्विस पारिस्थितिकी-तंत्र के अंदर केवल बीपीएच प्रोवाइडर्स ही ढांचा प्रोवाइडर्स की एकमात्र श्रेणी नहीं हैं। ये सेवाएं साइबर-अपराध अभियानों को सक्रियात्मक समर्थन देकर और जानबूझकर वैध जांच व प्रतिक्रिया को बाधित करके ऑस्ट्रेलिया के लिए साइबर-अपराध खतरे को बनाए रखती हैं और इसे सक्षम बनाती हैं। बीपीएच प्रोवाइडर्स के विरुद्ध कदम उठाने से इन सेवाओं की अतिसंवेदनशीलता और इनका उपयोग करने वाले दुर्भावनापूर्ण साइबरकर्मी प्रकाश में आते हैं।