“বুলেটপ্রুফ” হোস্টিং সরবরাহকারীঃ সাইবার অপরাধীদের অবকাঠামোর বর্মে ফাটল

সফল সাইবার অপরাধীরা নিরাপদ, সনাক্ত করা যায় না এমন এবং মজবুত অবকাঠামোর উপর নির্ভর করে। নেটওয়ার্কে ঢুকে পড়া, পরিচয় চুরি হওয়া, র‍্যানসমওয়্যার, অথবা অবৈধ ফোরামে ডেটা চুরি এবং বিক্রির প্রতিটি ঘটনার পিছনে রয়েছে নিরাপদ অবকাঠামো যা সাইবার অপরাধীদের কার্যক্রম পরিচালনা করতে এবং লুকিয়ে থাকতে সক্ষম করে।

তবে, সাইবার অপরাধীদের জন্য লুকিয়ে থাকা এবং ধরা ছোঁয়ার বাইরে থাকা ক্রমশ একটি চ্যালেঞ্জ হয়ে উঠছে। সরকার, আইন প্রয়োগকারী সংস্থা এবং বেসরকারী খাতের মধ্যে বৈশ্বিক অংশীদারিত্ব তাদের অনলাইনে গোপনে থাকাকে আরও কঠিন করে তুলছে। তদুপরি, খুব কম সাইবার অপরাধীরই নিজেদের সুরক্ষিত অবকাঠামো পরিচালনা এবং রক্ষণাবেক্ষণ করার জন্য প্রয়োজনীয় জ্ঞান ও দক্ষতা রয়েছে। সেজন্য তারা অবৈধ অবকাঠামো সরবরাহকারীদের সন্ধান করে যারা তাদের পক্ষ হয়ে এই পরিষেবাটি সরবরাহ করতে পারে, যার ফলে সাইবার অপরাধীরা তাদের শিকার ও লাভের দিকে মনোনিবেশ করতে সক্ষম হয়।

‘সাইবার ক্রাইম-অ্যাজ-এ-সার্ভিস’ বলতে বোঝায় এমন এক অবৈধ আন্ডারগ্রাউন্ড বাজারকে, যা বিভিন্ন ধরনের দুর্বৃত্ত সাইবার অপরাধীদের সহায়তা করার জন্য গড়ে তোলা হয়েছে। এই গোপন বাজারে ক্রমবর্ধমান এবং সদা পরিবর্তনশীল বিভিন্ন ধরনের ক্রয়যোগ্য সরঞ্জাম, পরিষেবা এবং তথ্য পাওয়া যায় যা অনলাইনে মানুষকে ঠকাতে সাইবার অপরাধীদের সহায়তা করে। সাইবার অপরাধীরা নেটওয়ার্কগুলিতে অ্যাক্সেস কিনতে পারে, সুরক্ষা ব্যবস্থা এড়াতে সক্ষম এমন সরঞ্জাম ক্রয় করতে পারে, এর পাশাপাশি ক্ষতিগ্রস্তদের বিরুদ্ধে ব্যবহার এবং ব্যক্তিগত তথ্য চুরি করার জন্য ম্যালওয়্যার কিনতে পারে। বুলেটপ্রুফ হোস্টিং (BPH) সরবরাহকারীরা এই বাস্তুতন্ত্রেরই একটি অংশ এবং তারা সাইবার অপরাধীদের জন্য সুরক্ষিত অবকাঠামোর যোগান দেয়। গুরুত্বপূর্ণ দিক হল একজন BPH সরবরাহকারী সরাসরি শত শত সাইবার অপরাধীকে বিশ্বজুড়ে ভিক্টিমদের নিশানা করায় সক্ষম করতে পারে।

“বুলেটপ্রুফ” হোস্টিং সরবরাহকারী কী?

সহজ কথায় বলতে গেলে BPH সরবরাহকারীরা সাইবার অপরাধীদের ভার্চুয়াল এবং/অথবা সত্যিকারের অবকাঠামো ভাড়া দেয়, যেখান থেকে সাইবার অপরাধীরা তাদের কার্যক্রম পরিচালনা করতে পারে। BPH সরবরাহকারীরা হল ইন্টারনেট অবকাঠামো পরিষেবাগুলির একটি নির্দিষ্ট শ্রেণি যা প্রতারকদের (সাইবার ক্রিমিনাল সহ) অবৈধ সামগ্রী হোস্ট করতে এবং ইন্টারনেটে তাদের কার্যক্রম চালাতে সক্ষম করে।

“বুলেটপ্রুফ” শব্দটি হল পুরোদস্তর মার্কেটিং এর ভাষা। বাস্তবে, এই পরিষেবাগুলির কার্যক্রম অন্যান্য অবকাঠামো সরবরাহকারীদের মতোই বাধাগ্রস্ত হওয়ার জন্য সমান ঝুঁকিতে থাকে। আসলে BPH সরবরাহকারীরা সক্রিয়ভাবে আইন প্রয়োগকারী সংস্থার নির্দেশাবলী এবং বিষয়বস্তু অপসারণের অনুরোধ উপেক্ষা করে এবং ভুক্তভোগীদের অভিযোগ ও সাবস্ক্রাইবারদের অনুরোধের প্রতি কোনও কর্ণপাত করে না। এর অর্থ সাইবার অপরাধীরা নিজেদের মধ্যে যোগাযোগ করতে পারে, অবৈধ ফোরাম এবং ওয়েবসাইট চালাতে পারে, ম্যালওয়্যার এবং ফিশিং প্রচারণা করতে পারে এবং আইন প্রয়োগকারী সংস্থা বা অন্যান্য অনুরোধের কারনে অপারেটর তাদের ইজারা বাতিল করে দেবে এমন কোনও আশংকা ছাড়াই অর্থ পাচার করতে পারে।

BPH সরবরাহকারীরা জেনেশুনেই সাইবার অপরাধের জগতে অংশ নেয় এবং আর্থিকভাবে অনুপ্রাণিত গুরুতর সাইবার অপরাধী সংগঠনকে সক্ষম করে তোলে। অপরাধীদের দ্বারা BPH সরবরাহকারীদের ব্যবহারের ফলে অস্ট্রেলিয়ার কিছু প্রতিষ্ঠান এবং তাদের গ্রাহকরা ক্ষতিগ্রস্ত হওয়ার মতো কিছু বড় ধরণের সাইবার নিরাপত্তাজনিত ঘটনা ঘটেছে। এই ঘটনাগুলোর পরিপ্রেক্ষিতে বেপরোয়া র‍্যানসমওয়্যার আক্রমণ, ডেটা চুরি এবং সংবেদনশীল তথ্য চুরির মত ঘটনা ঘটেছে।

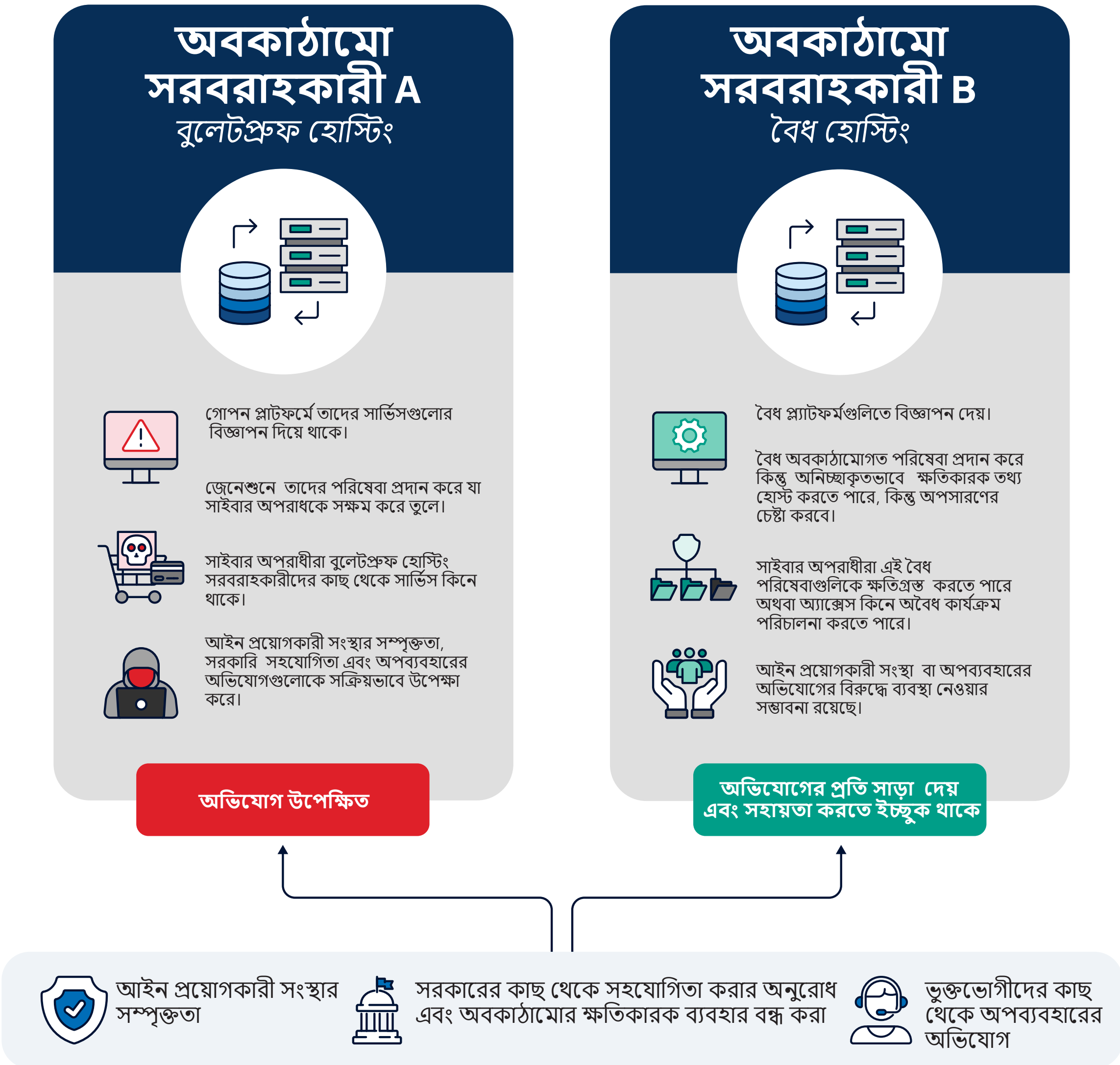
গোপন ফোরামে বুলেটপ্রুফ হোস্টিং সরবরাহকারীর বিজ্ঞাপনের উপস্থাপনা:

BPH সরবরাহকারীরা কিভাবে কাজ করে?

ভিন্ন ভিন্ন BPH সরবরাহকারীরা ভিন্ন ভিন্ন ব্যবসায়িক মডেল ব্যবহার করে। সবচেয়ে প্রচলিত পদ্ধতিটি হল সাইবার অপরাধীদের কাছে আইপি ঠিকানা ভাড়া দেয়া এবং নিজেদের অবস্থান, পরিচয় এবং কর্মকাণ্ড লুকানোর জন্য জটিল নেটওয়ার্ক পরিবর্তন পদ্ধতির ব্যবহার করা। বেশীর ভাগ ক্ষেত্রে, BPH সরবরাহকারীরা অন্যান্য বৈধ হোস্টিং সরবরাহকারী, ডেটা সেন্টার কিংবা ইন্টারনেট সার্ভিস প্রোভাইডারদের (ISPs) কাছ থেকে নিয়ে আইপি ঠিকানাগুলো পুনরায় বিক্রি কিংবা ভাড়া দিয়ে থাকে। এই ‘আপস্ট্রিম’ সরবরাহকারীরা হয়তো জানেই না যে তারা BPH সরবরাহকারীদের অবকাঠামো সরবরাহ করছে যারা পরবর্তীতে ‘ডাউনস্ট্রিমে’ সাইবার অপরাধীদের কাছে পরিষেবা দিচ্ছে।

BPH সরবরাহকারীরা তাদের নেটওয়ার্ক এবং সিস্টেম আর্কিটেকচারকে এমনভাবে সাজিয়ে নেয় যে তাদের গ্রাহকদের শনাক্ত করা অনেক কঠিন হয়ে পড়ে। উদাহরণস্বরূপ, তারা প্রায়ই ইন্টারনেটে তাদের গ্রাহকদের কর্মকাণ্ডের সাথে যুক্ত শনাক্তকারী তথ্য - যেমন তাদের নির্ধারিত আইপি ঠিকানা এবং ডোমেইন নেইম পরিবর্তন করে ফেলে। এই ধরনের কৌশলগুলি কোনও ঘটনার সাথে কোনও প্রতারক বা গ্রাহকের ব্যবহৃত আইপি ঠিকানার সংযোগ স্থাপনকে কঠিন করে তোলে, যার ফলে আইন শৃঙ্খলা রক্ষাকারী এবং তদন্তকারীরা চ্যালেঞ্জ এর মুখে পড়ে। এছাড়াও, বিপিএইচ (BPH) সরবরাহকারীরা প্রায়ই এমন দেশগুলোর অবকাঠামো ব্যবহার করে, যেসব দেশের সাইবার নীতিমালা শিথিল—যেখানে ক্ষতিকর সাইবার কার্যকলাপ তদন্ত ও প্রতিরোধে প্রাতিষ্ঠানিক ব্যবস্থা হয় অনুপস্থিত, নয়তো অত্যন্ত দুর্বল।

বৈধ অবকাঠামো সরবরাহকারীদের থেকে বুলেটপ্রুফ হোস্টিং সরবরাহকারীরা কিভাবে আলাদা হয়?



BPH সরবরাহকারীদের অনুসরণ করা যেভাবে সাইবার অপরাধের হুমকিকে ধ্বংস করে দেয়।

BPH সরবরাহকারীদের হাতে রয়েছে একবারে শত শত থেকে হাজার হাজার সাইবার অপরাধীদের কার্যক্রম ব্যাহত করার একটি মূল্যবান সুযোগ। বিভিন্ন ধরনের সাইবার অপরাধী এবং অন্যান্য সাইবার প্রতারকরা তাদের অপরাধকর্মকে সহজ করার জন্য এই পরিষেবাগুলি ব্যবহার করে - এটি বিশ্বাস করে যে প্রত্যাহারের অনুরোধ বা অপব্যবহারের অভিযোগের মুখে তাদের ক্রিয়াকলাপ গোপন এবং কার্যকর থাকবে।

তবে, আইন প্রয়োগকারী সংস্থা, সরকারী সংস্থা এবং বেসরকারী খাত পরিচিত BPH সরবরাহকারীদের কাছ থেকে সক্রিয়ভাবে ইন্টারনেট ট্র্যাফিক অবরুদ্ধ করার মতো প্রতিরক্ষামূলক ব্যবস্থা গ্রহণের মাধ্যমে এই অবৈধ অবকাঠামো সরবরাহকারীদের শনাক্ত ও তাদের ক্রিয়াকলাপ ব্যাহত করতে সহযোগিতা করছে। এই ক্রিয়াকলাপগুলি অস্ট্রেলিয়ান এবং অ্যালায়েড নেটওয়ার্কগুলির সাথে সাইবার অপরাধের মাত্রা হ্রাস করতে সহায়তা করে এবং বৈধ 'আপস্ট্রিম' অবকাঠামো সরবরাহকারী এবং ISPগুলিকে অন্তর্ভুক্ত করে যারা হয়তো না জেনেই BPH সরবরাহকারীদের ইন্টারনেট অ্যাক্সেস করতে এবং সাইবার অপরাধীদের সুরক্ষিত অবকাঠামো সরবরাহ করতে সক্ষম করে তোলে।

সাইবার ক্রাইম-অ্যাজ-এ-সার্ভিস ইকোসিস্টেমের মধ্যে BPH প্রদানকারীরাই একমাত্র অবকাঠামো সরবরাহকারী নয়। এই পরিষেবাগুলি সক্রিয়ভাবে সাইবার অপরাধমূলক প্রচারণাকে সহায়তা করে এবং ইচ্ছাকৃতভাবে আইনী তদন্ত ও পদক্ষেপকে বাধাগ্রস্ত করার মাধ্যমে অস্ট্রেলিয়ায় সাইবার অপরাধের হুমকিকে স্থায়ী ও সক্ষম করে তোলে। BPH সরবরাহকারীদের বিরুদ্ধে ব্যবস্থা নেওয়ার ফলে এই পরিষেবাগুলির দুর্বলতা এবং তাদেরকে ব্যবহারকারী সাইবার প্রতারকদের মুখোশ উন্মোচিত হচ্ছে।