

عنوان مقاله:

پدافند سایبری با بکارگیری تکنولوژی هانی پات

محل انتشار:

همایش تخصصی مهندسی دفاعی با عنوان «تهدیدات سایبرالکترونیک» (سال: 1400)

تعداد صفحات اصل مقاله: 9

نویسنده:

هادی نظرزاده - کارشناسی ارشد تجارت الکترونیک

خلاصه مقاله:

حملات پیشرفته ی سایبری، خطرهای جدی را برای اقتصاد و امنیت ملی کشورها پدید آورده است. امروزه کشورها استفاده از پدافند غیرعامل را در کنار پدافند عامل برای در امان ماندن از حملات سایبری به کار می برند. در دفاع غیرعامل سایبری، از نرم افزارها، حسگرها و جمع آوری اطلاعات برای تشخیص و توقف بدافزارها قبل از وقوع حمله استفاده می شود. با پیاده سازی صحیح راهکارهای فریب، تهدیدات امنیت سایبری رویکردی واکنش گرا و پویا به حملات و تهدیدات سایبری خواهد داشت و این رویکرد منجر به اعمال هزینه زیادی برای نفوذگران خواهد شد. یکی از روش های فریب استفاده از هانی پات است. در ساده ترین شکل هانی پات، یک سرور با اطلاعات راهبردی جعلی در شبکه است که به عنوان طعمه ای فریبنده با آسیب پذیری ساختگی برای جمع آوری اطلاعات مهاجمین و روش ها و اهداف آنها در شبکه قرار داده می شود. این ابزار فاقد اطلاعات ارزشمند است و لزوما هر تعاملی با آن بیانگر وقوع یک تهاجم در شبکه است. تله ها یا هانی پات ها، اهداف سناریوی بازی فریب تهدیدات سایبری می باشند. در این مقاله به بررسی کلی حمله و دفاع سایبری، تکنولوژی هانی پات، انواع هانی پات، مزایا و معایب هانی پات پرداخته می شود.

کلمات کلیدی:

پدافند الکترونیک، فریب، هانیپات، پدافند سایبری

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1380893>

