عنوان مقاله:
روشهای مقاومت در برابر حذف و مخفی شدن روت کیت های لایه هسته در حملات سایبری

محل انتشار:
کنفرانس بین المللی افق های نو در علوم مهندسی (سال: 1396)

تعداد صفحات اصل مقاله: 11

نویسندگان:
مهدی قربانی فر - *کارشناس تحلیلگر سیستم، دانشگاه علوم پزشکی قم، ایران*

عادله بیگدلی - *کارشناس ارشد مهندسی کامپیوتر، گرایش نرم افزار دانشگاه آزاد اسلامی آشتیان، ایران*

خلاصه مقاله:
اطمینان از امنیت سیستم های کامپیوتری در عصر مدرن امروزی بسیار دشوار است و راه های زیادی برای نفوذ عوامل مخرب به یک سیستم، به دست آوردن کنترل و حفظ این کنترل وجود دارد.یکی از این راه ها استفاده از روت کیت ها می باشد که روت کیت یک نوع بدافزار است که به صورت مخفیانه وارد سیستم کامپیوتری میزبان می شود و یک دریچه در آن برای بدافزارهای دیگر برای تهدیدات بیشتر میزبان باز می کند. قابل ذکر است که انواع مختلفی از روت کیت ها وجود دارد از جمله روت کیت هایی که سخت افزار را تحت تاثیر قرار می دهند، تنها در حافظه اجرا می شود و یا کلا در لایه کاربر باقی می مانند. این مقاله بر روت کیت های لایه هسته تمرکز می کند که اساسا از طریق دستکاری در هسته یا ویژگی سیستم و منابع مرتبط عمل می کنند. برای اینکه روت کیت ها بتوانند به عنوان یک روش مفید باقی بمانند، هر کاری برای تضمین استقامت و پایداری خود انجام خواهند داد، ترکیب بندی را تغییر میدهند و یا حتی این ترکیب بندی را مستقیما حذف خواهند کرد. این کار از طریق مخفی کردن فایل ها، فرایندها و حتی ادقام به یک سیستم طوری که حذف از آن باعث خرابی کل سیستم میشود، انجام خواهد شد و مهمترین وظیفه هر روت کیت استقرار در سیستم قربانی بدون شناخته شدن است. روت کیت هر کاری برای مخفی نگه داشتن حضورش از فهرست های پردازش و ساختار دایرکتوری انجام میدهد و حتی تلاش میکند تا برنامه هایی که میداند ممکن است باعث به خطر افتادن حضورش و یا حذف آن شود از کار می اندازد. بخشی از مقاومت و ایستادگی روت کیت به توانایی آن برای مخفی شدن بستگی دارد. روت کیت ها از چندین تکنیک برای مخفی نگه داشتن شواهد فیزیکی و شواهد فرایندخود از سرویس هایی که ممکن است فعالیت مخرب را شناسایی کنند، استفاده می کنند.

کلمات کلیدی:
روت کیت ، روت کیت های لایه هسته ، استقامت در برابر حذف ، شواهد فیزیکی ، شواهد فرایند