کنگره بین المللی علوم و مهندسی
آلمان – هامبورگ
اسفند ماه ۱۳۹۶

بررسی نقاط قوت و ضعف عمومی‌ترین روش‌های موجود در مقابله با باج‌افزارها

فرهنگ پدیداران مقدم[۱]، سعید آقایی[۲]، مهشید صادقی باجگیران[۳]

۱- استادیار گروه کامپیوتر، موسسه آموزش عالی اشراق بجنورد padidaran@eshragh.ac.ir
۲- دانشجوی کارشناسی ارشد مهندسی نرم افزار، موسسه آموزش عالی اشراق بجنورد
saeed.aghaee.88@gmail.com
۳- دانشجوی کارشناسی ارشد مهندسی نرم افزار، موسسه آموزش عالی اشراق بجنورد
m.sadeghi.daraee@88@gmail.com

چکیده

در دنیای امروز، با ارزش ترین چیزی که در هر سازمان یا شرکت نگه داری می شود، اطلاعات دیجیتالی آنهاست، و با توجه به ارزش بالای این اطلاعات، همیشه سازمان ها و شرکت ها اهداف خوبی برای باج‌افزارها بوده اند، در حال حاضر روش های متفاوتی برای مقابله با باج‌افزار[۱]وجود دارد که هریک مشکلات خود را داشته و بدلیل جدید بودن این بدافزار ها، هنوز روش کاملی مورد استفاده قرار نگرفته است. در این مقاله ما ۴ روش مرسوم مقابله با باج‌افزار شامل CLD Backup که جهت مقابله با باج‌افزار در زمان بکاپ‌گیری، روش های Multilayered Defense و Antiransomware که روش های عمومی مقابله و تشخیص می باشند، روش کنترل دسترسی که در سیستم عامل بکار می رود و در نهایت روش KeyBackup که جهت بازگردانی اطلاعات رمزگذاری توسط باج‌افزار می باشد را مورد بررسی قرار داده و ایرادها و نقاط قوت هریک را عنوان می نماییم، که بطور کلی میتوان گفت مهمترین نقاط ضعف موجود، وابستگی اکثر روش های فعلی مقابله با باج-افزار به پلتفرم[۲]خاص و مشکل سربار ناشی از مانیتورینگ[۳]و مشکل خطای مثبت شناسایی[۴] می باشد، در نتیجه روشی که کمترین سربار و خطای مثبت شناسایی را داشته باشد و به پلتفرم خاصی وابسته نباشد قطعا بهترین روش ممکن خواهد بود.

واژه‌های کلیدی: باج افزار، بازیابی داده ها، کلید رمزگذاری، دفاع چند لایه ای، کنترل دسترسی

[1] Ransomware
[2] Platform
[3] Monitoring
[4] False-Positive