عنوان مقاله:
مروری بر تاریخچه، ساختار، روش های پیشگری و مقابله با باج افزارها

محل انتشار:
سومین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 9

نویسندگان:
ابراهیم سیاحی - *کارشناس ارشد امنیت اطلاعات، آزمایشگاه و مرکز تخصصی آپا، دانشگاه شیراز، شیراز،*

مهرداد فرخ منش - *کارشناس ارشد امنیت اطلاعات، آزمایشگاه و مرکز تخصصی آپا، دانشگاه شیراز، شیراز،*

مریم باصری - *کارشناس ارشد فناوری اطلاعات، آزمایشگاه و مرکز تخصصی آپا، دانشگاه شیراز، شیراز،*

علی حمزه - *دانشیار، آزمایشگاه و مرکز تخصصی آپا، دانشگاه شیراز، شیراز،*

خلاصه مقاله:
باج افزارها یکی از مهمترین چالش های امنیتی در سال های اخیر هستند. باج افزار نوعی از بدافزار است که تلاش می کند با ایجاد نوعی اختلال در دسترسی کاربران به اطلاعات و یا منابع سیستم، مبلغی باج را در ازای بازگرداندن دسترسی به اطلاعات و منابع از کاربر درخواست کند. یکی از مهمترین دلایل رشد و محبوبیت اینگونه از بدافزارها، ظهور پول های الکترونیکی و شبکه های مخفی اینترنتی نظیر Tor بوده است. پول های الکترونیکی نظیر بیت کوین، امکان انتقال پول را در حالی می دهد که فرستنده و گیرنده ناشناس هستند. همچنین سرورهای موجود در شبکه Tor به راحتی قابل شناسایی و مسدود سازی نخواهند بود. در سال های اخیر دسترسی به باج افزار برای حمله به یک هدف راحت تر شده است بطوری که برخی منابع باج افزار را بصورت سرویس ارایه می کنند و افراد می توانند با پرداخت مبلغی پول، باج افزار دلخواه خود را سفارش دهند. با سفارش یک باج افزار تنها کاری که باقی می مانند پخش کردن آن و آلوده سازی سیستم قربانی است. در این مقاله ابتدا مروری بر تاریخچه باج افزارها و میزان پیشرفت آنها در سال های اخیر خواهیم داشت. سپس ساختار کلی باج افزار و نحوه کار آنها را بررسی خواهیم کرد و در ادامه راهکارهایی را به منظور پیشگیری از ابتلا به باج افزار و همچنین مقابله با آنها ارایه خواهیم کرد.

کلمات کلیدی:
باج افزار، رمز کننده، قفل کننده، Petya ، Wannacry ، CryptoLocker