شنبه 01 اردیبهشت 1397 - 15:23

توصیه های امنیتی در مورد بد افزار Stuxnet

بدافزار Stuxnet

اخیراً یک بدافزار خطرناک به نام Stuxnet در همه کشورهای جهان و به خصوص ایران گسترش پیدا کرده است که هدف آن ایجاد اختلال در شرکت ها و سازمان های مرتبط با زیرساخت های حیاتی همچون نیروگاه ها است. بدافزار مذکور با سوءاستفاده از یک حفره امنیتی در ویندوز گسترش پیدا می کند و به دنبال سیستم هایی است که از نرم افزار WinCC Scada که متعلق به زیمنس است، استفاده می کنند. نرم افزار مذکور معمولاً توسط سازمان های مرتبط با زیرساخت های حیاتی مورد استفاده قرار می گیرد.

بنا بر اطلاعات ارائه شده توسط سایمانتک، کرم رایانه ای Scada که هدف آن شرکت ها و سازمان های مربوط زیرساخت های حیاتی هستند، نه تنها به سرقت اطلاعات می پردازد، بلکه یک back door را نیز بر روی سیستم قربانی قرار می دهد تا بتواند از راه دور و به طور مخفیانه کنترل عملیات زیرساخت های مذکور را در اختیار گیرد.

کرم Stuxnet، شرکت های مربوط به سیستم های کنترل صنعتی در سراسر جهان را آلوده ساخته است، با این وجود بنا بر گزارش های دریافت شده، بیشتر آلودگی ها در ایران و هند مشاهده شده است.

فایل های MD5

ابزار رفع بدافزار stuxnet:

ابزار مرکز آپای شریف جهت رفع بدافزار stuxnet

ابزار مرکز آپای امیرکبیر جهت رفع بدافزار stuxnet

اصلاحیه های مایکروسافت:

ms10-046
ms10-061
ms10-067

منبع :www.certcc.ir