یکشنبه 03 مرداد 1389 - 09:17

حمله یک ویروس خطرناك به رایانه‌هاي ایراني

پایگاه اینترنتي PCworld در مطلبي نوشت: رایانه هاي ایران به شدت هدف حمله SCADA worm، یکي از خطرناکترین کرم هاي (ویروس) رایانه اي قرار گرفته اند که به منظور سرقت اطلاعات از سامانه هاي کنترل صنعتي طراحي شده است...

پایگاه اینترنتي PCworld در مطلبي نوشت: رایانه هاي ایران به شدت هدف حمله SCADA worm، یکي از خطرناکترین کرم هاي (ویروس) رایانه اي قرار گرفته اند که به منظور سرقت اطلاعات از سامانه هاي کنترل صنعتي طراحي شده است.
به گزارش واحد مرکزي خبر، بنابر اعلان موسسه Symantec نزدیک به شصت درصد از همه رایانه هاي آلوده به این کرم ویروس در ایران قرار دارند.
اندونزي و هند نیز از جمله کشورهایي هستند که به شدت هدف حمله این ویروس موسوم به Stuxnet قرار گرفته اند.
الیاس لوي مدیر فني موسسه Symantec Security Response گفت: این نرم افزار ویروسي از ماه ژانویه فعال شده است.
این ویروس را ماه گذشته شرکت آنتي ویروس VirusBlokAda بلاروس شناسایي کرد.
این شرکت اعلام کرد این ویروس را روي رایانه اي شناسایي کرده است که به یکي از مشتریان ایراني این شرکت تعلق داشت.
این ویروس به دنبال سیستم هاي نظارت مدیریتي و مبادله داده زیمنس مي گردد که عمدتا براي نظارت و یا کنترل فرایندهاي شیمیایي و یا حمل و نقلي در شبکه هایي نظیر تامین آب شهري، کنترل نیروي برق، انتقال و توزیع آن، لوله هاي گاز و نفت و بسیاري پروسس هاي توزیع شده دیگر استفاده مي شوند.
Symantec Security Response مطمئن نیست که چرا در ایران و کشورهاي دیگر رایانه ها به تعداد بسیار زیادي به این ویروس آلوده شده اند.
لوي افزود : "بیشترین چیزي که ما مي توانیم بگوییم این است هدف طراحان این ویروس، مخصوصا کشورهایي است که در آن محدوده جغرافیایي قرار دارند."
وي ادامه داد "هرچند ایران احتمالا یکي از کشورهایي است که بیشترین موارد آلودگي رایانه ها به این ویروس در آن گزارش شده است ولي این کشورها جزو آن دسته از کشورها هستند که آنتي ویروسهاي زیادي ندارند."
زیمنس نمي گوید که چه تعداد مشتري داراي سیستم SCADA در ایران دارد ولي اذعان دارد که دو شرکت آلماني نیز مورد حمله این ویروس قرار گرفته اند.
به نوشته روزنامه وال استریت ژورنال، زیمنس چند ماه پیش اعلام کرد در نظر دارد فعالیت دو واحد تولیدي خود را در ایران کاهش دهد.
یکي از این واحدها، دویست و نود کارمند دارد و در سال دو هزار و هشت میلادي به سود خالص چهارصد و سي و هشت میلیون یورو معادل پانصدو شصت و دو میلیون و نهصد هزار دلار دست یافت.
به گفته لوي، طي یک دوره سه روزه در هفته کنوني، رایانه هاي مستقر در چهارده هزار IP سعي کردند به سرورهاي فرمان و کنترل متصل شوند. این امر نشان مي دهد که تعداد رایانه هاي آلوده به ویروس SCADA در جهان خیلي کم است و احتمالا حدود پانزده تا بیست هزار رایانه به این ویروس آلوده شده اند ، زیرا بسیاري از شرکت ها چند رایانه را در یک نشاني IP قرار مي‌دهند.
از آنجایي که شرکت Symantec مي تواند IP هاي دستگاههاي را که سعي مي کنند به سرورهاي فرمان و کنترل وصل شوند، شناسایي کند در نتیجه مي تواند تشخیص دهد که کدامیک از شرکت ها آلوده به این ویروس شده اند.
رکت Symantec پنجشنبه گذشته در پایگاه اینترنتي خود اعلام کرد دستگاههاي آلوده به ویروس SCADA به سازمان هایي تعلق دارند که از نرم افزار و سیستم هاي SCADA استفاده مي کنند.
ویروس SCADA یا Stuxnet از طریق پورت یو اس بي گسترش مي یابد.زماني که ابزاري آلوده به این شکل به رایانه اتصال پیدا مي کند، کدهاي آن به جستجوي سیستمهاي زیمنس گشته و خود را بر روي هر ابزار یو اس بي دار دیگري که بیابد، کپي خواهد کرد.
ین ویروس جدید اینترنتي براي سرقت اطلاعات حساس شرکت هاي صنعتي طراحي شده است.
بر اساس هشدار شرکت زیمنس ویروس یاد شده بسیار پیچیده بوده و رایانه هایي را هدف مي گیرد که براي مدیریت سیستم هاي کنترل صنعتي در مقیاس وسیع مورد استفاده قرار مي گیرند.
این ویروس به خصوص سیستم هایي را هدف مي گیرد که توسط شرکت هاي طراح و سازنده قطعات مختلف صنعتي به کار گرفته مي شوند.
یمنس اعلام کرده گروهي کارشناس را براي ارزیابي وضعیت و مقابله با تحرکات این ویروس آماده کرده است.
زیمنس همچنین مجموعه هاي صنعتي مرتبط با خود را در جریان عملکرد این ویروس قرار داده و آنها را از خطرات بالقوه آن مطلع نموده است. برخي نگرانند که این ویروس در آینده پیچیده تر شود و عملیات شرکت ها و کارخانه ها را مختل کند.