نحوه جلوگیری از آلوده شدن به باج افزار جدید WANNACRY

واحد خدمات پس از فروش شرکت پایا افزار

۱۳۹۶/۰۲/۲۶

آشنایی با باج افزار Wannacry

روز جمعه بیش از ۷۰ هزار کامپیوتر در سراسر جهان به یک باج افزار آلوده شدند. سازمان ملی بهداشت انگلیس و چندین بیمارستان در همین کشور ، یک شرکت مخابراتی در اسپانیا ، دفاتر فدکس در انگلیس ، چند بانک در سراسر دنیا و حتی بر اساس گزارشات وزارت کشور روسیه در میان سیستم های قربانی بوده اند.

هکرها از حفره « EternalBlue» که در ویندوز وجود داشته استفاده کرده اند. حفره ای که گفته می شود سازمان NSA پیشتر از آن برای دور زدن امنیت ویندوز بهره گرفته. حفره ای که مایکروسافت دو ماه پیش آن را در یکی از به روز رسانی های ویندوز رفع کرده اما طبق معمول همه به سرعت آپدیت نمی کنند و کامپیوترهایی که قربانی باج افزار شده اند از نسخه های قدیمی تر ویندوز استفاده کرده اند. (جدا از۸,۴۵ درصد کاربران ویندوز که هنوز از اکس پی استفاده می کنند و مایکروسافت دیگر از آنها پشتیبانی نمی کند).

ماجرا به شکل خلاصه از این قرار بوده: هکرهای گمناک که هنوز هویت شان مشخص نیست ویروسی طراحی کرده و با آن سرورهای مجهز به نرم افزار مایکروسافت که پروتکل اشتراک فایل « Server Message Block» را اجرا می کرده را هدف قرار داده اند. تنها سرورهایی که به پچ ارائه شده در چهاردهم مارس یعنی «MS17-010» آپدیت نبودند به باج افزار آلوده می شوند

این باج افزار که «WannaCrypt0r 2.0» (به اختصار WannaCry - میخواهی گریه کنی) نام دارد فایل های مهم در کامپیوتر قربانی را رمزگذاری می کند و سپس به کاربر اجازه استفاده از کامپیوتر را نمی دهد تا در نهایت مبلغی به عنوان باج برای گشودن فایل ها از سوی کاربر پرداخت شود.

نحوه جلوگیری از آلوده شدن به باج افزار wannaCry

برای جلوگیری از آلوده شدن در برابر باج افزار که به سرعت در حال تکثیر است ، کافی است موارد زیر را رعایت فرمایید :

- به روز رسانی سیستم عامل های ویندوز

- پشتیبان گیری از اطلاعات مهم و حیاتی سیستم ها (فایلهای پشتیبان نرم افزار ها به همراه فولدرهای معرفی شده)

- به روز رسانی آنتی ویروس ها و اطلاع رسانی به کاربران جهت عدم اجرای فایل های پیوست ایمیل های ناشناس

- غیر فعال سازی پروتکل SMB در سیستم عامل در صورت عدم به روز رسانی یا نصب وصله ها

https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

- بستن پورتهای ۱۳۹ و ۴۴۵ از طریق فایروال (سخت افزاری و فایروال ویندوز)

- خودداری از باز کردن ایمیل ها مشکوک و ناشناس

- نصب وصله MS17-010 از لینک زیر :

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

- غیر فعال کردن مایکروها

- در خصوص سیستم عاملهای ویندوز xp و سرور ۲۰۰۳ که End of Support شده اند نیز مایکروسافت وصله اختصاصی در لینک زیر قرار داده است

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598