بسمه تعالی

اقدامات عملی جهت پیشگیری و مقابله با باج‌افزار wannacrypt

مرکز آپا دانشگاه اراک

اردیبهشت ۱۳۹۶

۱. باج افزار Wannacry چیست؟

فایل هـای موجـود بـر روی رایانـه کـاربر را قفـل (رمزنگـاری) مـی کنـد و در ازای بـاز گردانـی آنهـا تقاضای پرداخت باج می کند.

۲. نحوه عملکرد Wannacry:

از یک آسیب پذیری موجود در سیستم عامل ویندوز مایکروسافت برای نفوذ استفاده می کند.

از طریق شبکه

پیوست های ایمیل

بازدید سایت های آلوده

۳. آیا سیستم ما آلوده شده است؟

با نمایش پیغامی مبنی بر درخواست باج خواهی، متوجه خواهید شد که سیتم آلوده شده است و تمام اطلاعات رمز شده اند.

۴. اقدامات لازم پس از آلوده شدن؟

خاموش نمودن سیستم

قطع ارتباط شبکه

تماس با مرکز فناوری اطلاعات مربوطه

تماس با مرکز آپا دانشگاه اراک

اسکن سیستم با آنتی ویروس بروز شده

باز گردانی فایل ها با استفاده از نسخه های پشتیبان استفاده از System Restore سیستم عامل

۵. نام های مختلف باج افزار

WannaCry

Wanna Decrypt0r

WannaCryptor

WCRY

۶. اقدامات پیشگیرانه

۱-اجتناب از بازکردن و اجرای پیوست های ایمیل های ناشناخته

۲-بروز رسانی ویندوز

۳- بروز رسانی آنتی ویروس

۴- نصب وصله MS17-010

برای ویندوز دسکتاپ ۸,۱ و بالاتر :

۱) ابتدا Control Panel ویندوز را باز کنید بر روی Programs and Features کلیک کرده و روی گزینه Turn Windows features on or off کلیک کنید.

۲) از پنجره باز شده SMB1.0/CIFS File Sharing Support تیک Checkbox این سرویس را برداشته و OK را بزنید تا پنجره بسته شود.

۳) ویندوز را ریستارت کنید.

حتما توصیه می شود بعد از غیرفعال سازی سرویس SMB ویندوز را به آخرین نسخه به روز رسانی کرده و مجددا راه اندازی کنید.

اگر از حدود ۲ ماه پیش (۱۴ مارچ) تا حالا ویندوز هاتون رو آپدیت نکردین برای تکثیر نشدن باج افزار wanna cry ابتدا به سایت زیر مراجعه کنید:

http://www.catalog.update.microsoft.com/Home.aspx

بعد برای ویندوز R۲۲۰۰۸ و ویندوز ۷ چه ۳۲ بیت و چه ۶۴ بیت آپدیت شماره ۴۰۱۲۲۱۲ رو ابتدا در این سایت سرچ کنید و هر کدام را جدا گانه دانلود و نصب نمایید.

برای ویندوز R۲۲۰۱۲ شماره ۴۰۱۲۲۱۳

برای ویندوزهای دیگر با ورژن متفاوت رو هم می تونین شماره آپدیت رو از سایت زیر بدست بیاورید:

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

مرکز آپا دانشگاه اراک

Apa.araku.ac.ir

شماره های تماس مرکز :

۰۸۶ ۳۲۶۲ ۲۲۹۰

۰۸۶ ۳۲۶۲ ۲۲۹۲