گزارش هک گسترده باج افزار WannaCrypt در سراسر جهان و روش پیشگیری از آن

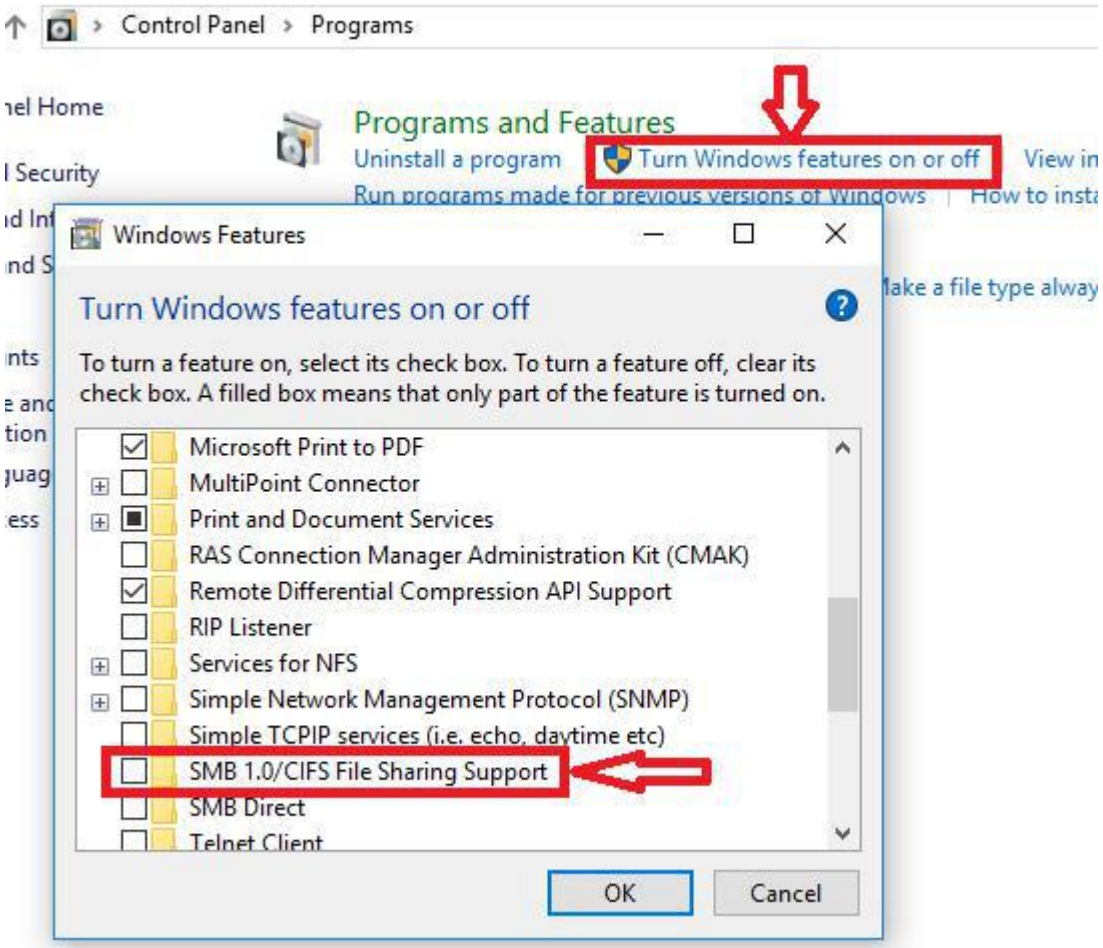
مقدمه

همان گونه که پلیس فتا نیز هشدار داده است، باج افزار WannaCrypt بطور گسترده در کشورهای متعددی سیستمها و فایلهای کاربران را دچار مشکل کرده است . در کشور ما نیز تا امروز بیش از ۲۰۰ سازمان به آن آلوده شده اند که مبلغ ۳۰۰ تا ۶۰۰ دلار را برای باز کردن رمز فایلها مطالبه می کند مطلب زیر به معرفی این باج افزار و راه مقابله با آن که به روزرسانی ویندوز است اختصاص دارد . ابتدا بطور سریع راههای پیشگیری مطرح می گردد.

راههای پیشگیری

بهتر است ابتدا سرویس SMB ویندوز را غیرفعال کنید که از طریق Control Panel طبق شکل زیر انجام می‌شود:

گزارش هک گسترده باج افزار WannaCrypt در سراسر جهان و روش پیشگیری از آن



برای ویندوز ۷ باید خط فرمان cmd را در حالت admin اجرا کنید و دو دستور زیر را در محیط آن اجرا نمایید:

sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi

sc.exe config mrxsmb10 start= disabled

اما موثرترین اقدام پیشگیرانه، به روز رسانی ویندوز است . کاربرانی که به طور مستمر ویندوز خود را به روزرسانی می کنند، ماه قبل در برابر این باج افزار ایمن شده اند . اگر هنوز اقدام نکرده اید، باید به روز رسانی MS17-010 را نصب کنید. کافی است نوع ویندوز خود را از لینک زیر انتخاب نموده و نصب نمایید:

گزارش هک گسترده باج افزار WannaCrypt در سراسر جهان و روش پیشگیری از آن

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx?f=255&MSPPError=-2147217396

برای ویندوز xp نیز از لینک زیر استفاده نمایید:

https://t.co/KxpdJCujE7?amp=1

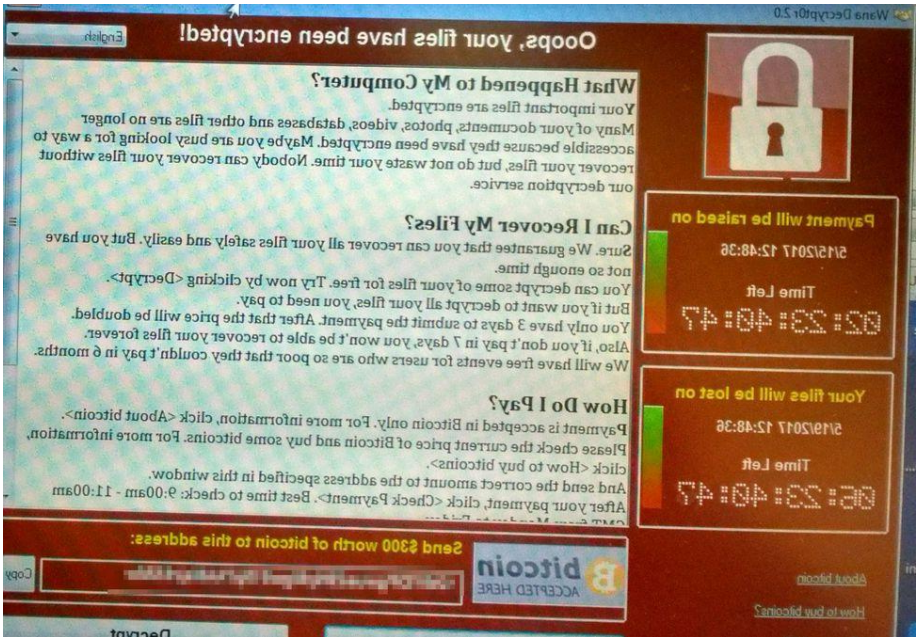
معرفی و گستره عمل باج افزار

سایت دیجیاتو – 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 از ۸.۴۵ 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 گمنام 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.

گزارش هک گسترده باج افزار WannaCrypt در سراسر جهان و روش پیشگیری از آن



این باج افزار که («WanaCrypt0r 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.

مبلغ درخواستی از سوی هکرها برای باز کردن هر کامپیوتر حدود ۳۰۰ دلار)توسط بیت کوین) ذکر شده. هکرها همچنین تهدید کرده اند که بیمارستان ها تا ۱۵ مه (پس فردا) فرصت دارند تا مبلغ درخواستی را پرداخت کنند. در غیر این صورت، تمام فایل هایی که رمزگذاری شده اند تا ۱۹ مه حذف خواهند شد.

سازمان ملی بهداشت انگلیس (NHS) که یکی از قربانیان اصلی این هک است، خبر داده که اطلاعات خصوصی مربوط به بیماران به سرقت نرفته است . برخی کارشناسان خبر داده اند که هنور تعداد زیادی از کامپیوترهایNHS ، از ویندوز اکس پی مایکروسافت استفاده کرده و به هیچ عنوان امن نیستند . در بیانیه خود NHS هم آمده که تا کنون ۱۶ بیمارستان در انگلیس به این باج افزار آلوده شده اند . این شرایط در بیمارستان های انگلیس وضعیتی اضطراری را رقم زده و باعث لغو شدن بسیاری از قرارهای ملاقات بیماران با

گزارش هک گسترده باج افزار WannaCrypt در سراسر جهان و روش پیشگیری از آن

پزشکان شده، در حالی که کارکنان بیمارستان ها قادر به استفاده از کامپیوترهای خود برای دسترسی به پرونده ها برای رسیدگی به بیماران نیستند.

گفته می شود که این نوع حملات از سال ۲۰۱۵ تا کنون افزایش قابل توجهی داشته اند . در سال ۲۰۱۵، ۳۴۰ هزار حمله توسط باج افزار ثبت شده در حالی که در سال ۲۰۱۶، تعداد این نوع حملات به ۴۶۳ هزار رسیده، هر چند تعداد حملاتی در این سطح، به ندرت اتفاق می افتد و بر اساس آخرین گزارش ها، تا کنون این باج افزار در ۹۹ کشور تاثیر خود را گذاشته است.

برای جلوگیری از به وجود آمدن این مشکل برای کامپیوتر خودتان، آخرین به روز رسانی مایکروسافت برای ویندوز را دریافت و نصب کنید.

منبع:

http://digiato.com/article/2017/05/13/%d9%87%da%a9-da%af%d8%b3%d8%aa%d8%b1%d8%af%d9%87-%d8%a8%d8%a7%d8%ac-%d8%a7%d9%81%d8%b2%d8%a7%d8%b1-wannacry-%d8%af%d8%b1-%d8%b3%d8%b1%d8%a7%d8%b3%d8%b1-%d8%ac%d9%87%d8%a7%d9%86%d8%9b-%d8%b4%d8%b1 /

جدول ۱ : تاریخچه سند

نسخه	ویرایش	تاریخ	توضیحات
1.0	فروغ هنرور	۹۶/۲/۲۳	معرفی باج افزار
1.1	ناصر قدیری	۹۶/۲/۲۴	راهکارهای مقابله