گزارشِ تحقیق درباره‌ی نحوه‌ی کارکرد اکسپلویتِ EternalBlue و باج‌افزارِ WannaCry

تهیه و تنظیم: مبین خیری

شماره دانشجویی: 994421017

استاد راهنما: دکتر میرسامان تاجبخش

چکیده:

در گزارشِ پیش‌رو قصد داریم نحوه‌ی عملکردِ باج‌افزارِ WannaCry و نیز ویژگی‌های مختلفِ آسیب‌پذیریِ EternalBlue را بررسی کنیم. این گزارش با استفاده از منابعِ پرشمارِ موجود در سطحِ اینترنت تهیه و تنظیم شده است.

باج‌افزار WannaCry چیست؟

تقریباً همهٔ افرادی که با اینترنت سروکار دارند، کم و بیش با Ransomware (باج‌افزار) آشنا هستند. مسئلهٔ باج‌افزارها موضوعی نیست که بتوان آن را نادیده گرفت یا به سادگی از آن عبور کرد زیرا همواره این خطر وجود دارد که اطلاعات مهم و حساس شما توسط این بدافزارها قفل شده و از دسترس‌تان خارج شوند و سپس به منظور باجگیری و اخاذی از شما، مورد استفاده قرار گیرند. در این میان، باج‌افزاری به نام WannaCry با سرعت فوق‌العاده‌ای میلیون‌ها کاربر را در سطح جهان آلوده نموده و با اتصال دیواس‌های متعدد به اینترنت، انتظار می‌رود لحظه به لحظه فراگیرتر نیز بشود و از همین روی شاید لازم باشد خود را برای مقابله با بدترین شرایط آماده کنید. در همین راستا، در این مقاله به ماهیت باج‌افزار WannaCry و نحوهٔ محافظت از اطلاعات در مقابل آن خواهیم پرداخت.

WannaCry چیست و چه کسی آن را ایجاد کرد؟

گروهی از هکرها تحت‌عنوان ShadowBrokers این باج‌افزار را منتشر کرده و قدرت تخریب نهفته در WannaCry نخستین بار توسط NSA (آژانس امنیت ملی آمریکا) شناسایی شد. شرکت‌های بزرگ نرم‌افزاری تولیدکنندهٔ سیستم‌عامل مانند مایکروسافت، گوگل و اپل هم بلافاصله دست به کار شده و شروع به رفع معایبی نمودند که می‌توانست توسط WannaCry مورد سوءاستفاده قرار گیرد اما هکرها نیز بیکار ننشستند و نسخهٔ جدیدی از این Malware (بدافزار) را تولید کردند تا بتوانند کامپیوترها و دیوایس‌های بیشتری را مورد حمله قرار دهند.

باج‌افزار WannaCry می‌تواند کامپیوترهایی که به اینترنت متصل می‌شوند را مورد حمله قرار داده و با رمزنگاری، اطلاعات را از دسترس صاحبان آن‌ها خارج نماید. در واقع، با این کار صاحبان فایل‌ها هیچ راهی برای رمزگشایی دیتای خود نخواهند داشت و این آهرم بسیار قدرتمندی در دست هکرها است تا در ازای

رمزگشایی فایل‌ها و دسترسی مجدد به آن‌ها، صاحبان فایل‌ها را مورد باج‌گیری و اخاذی قرار دهند (به خاطر همین باج‌خواهی است که این بدافزار، باج‌افزار نامیده شده است.)

این روزها با افزایش ظرفیت هارددیسک‌ها از یکسو و همچنین حجم بالای داده‌ها از سوی دیگر، بسیاری از افراد داده‌های زیادی را جمع‌آوری نموده و بر روی هارددرایو خود ذخیره می‌کنند؛ اما اگر کامپیوتر شما مورد حمله قرار گرفته و فایل‌ها قفل شوند، برای دسترسی مجدد به آن‌ها هیچ چاره‌ای برایتان به جز باج دادن به هکرها باقی نمی‌ماند (البته راه دیگری هم به جز باج دادن هست اما طرفداران زیادی ندارد زیرا بسیار دشوار بوده و خود مصیبت دیگری است و آن هم اینکه فایل‌ها و اطلاعات قفل شده را فراموش نموده و از صفر شروع کنید!)

چه کسانی تحت تأثیرات مخرب باج‌افزار WannaCry قرار می‌گیرند؟

می‌توان گفت هر کسی که به اینترنت وصل می‌شود به طور بالقوه در معرض حملهٔ این بدافزار قرار دارد اما این خطر صدها سازمان و میلیون‌ها کاربری که هنوز هم از سیستم‌عامل‌های قدیمی و منسوخ‌شده استفاده می‌کنند را بیشتر تهدید می‌کند. اکثر قربانیان این بدافزار کاربرانی هستند که، حتی پس از اینکه مایکروسافت به‌روزرسانی دوره‌ای نرم‌افزارها و آپدیت‌های امنیتی ویندوز XP را متوقف کرد، هنوز هم از ویندوز XP استفاده می‌کنند!

توقف تصادفی WannaCry با استفاده از Kill Switch و انتشار نسخهٔ جدید آن

یکی از محققان امنیتی کمپانی MalwareTech، به طور تصادفی و با استفاده از یک Kill Switch موفق شد فعالیت WannaCry را متوقف کند؛ اما پس از انجام این Kill Switch، هکرها توانستند نسخهٔ جدیدی از این بدافزار را تحت‌عنوان WannaCry 2.0 منتشر کنند و این در حالی است که این نسخهٔ جدید و پیشرفته را نمی‌توان با همان Kill Switch قدیمی متوقف کرد. تنها پس از اینکه ماهیت نسخهٔ اولیه شناسایی شود، هکرهایی که به‌اصطلاح Ethical Hacker (هکر اخلاق‌مدار) نامیده می‌شوند، قادر خواهند بود تا به مقابله با این بدافزار بپردازند.

چرا هکرها باج را به صورت بیتکوین درخواست می‌کنند؟

اینکه هکرها باج را به صورت بیتکوین درخواست می‌کنند حرکتی هوشمندانه در جهت حفظ امنیت و بقای خود است. فرض کنید هکرها می‌خواستند اطلاعات حساب بانکی خود را برای واریز وجه در اختیار قربانیان قرار دهند که در این صورت بلافاصله شناسایی می‌شدند و دیگر نمی‌توانستند به باج‌گیری خود ادامه دهند.

آیا حملهٔ WannaCry همچنان ادامه خواهد داشت؟

متأسفانه بایستی گفت آری! با انتشار نسخهٔ جدید WannaCry موسوم به WannaCry 2.0، این بدافزار قادر خواهد بود تا میلیون‌ها کاربر دیگر را نیز تحت‌تأثیر قرار دهد و در حال حاضر راهی برای متوقف کردن و جلوگیری از گسترش آن وجود ندارد.

چگونه امنیت خود را در مقابل WannaCry حفظ کنیم؟

اولین و مهم‌ترین کاری که باید بکنید این است که فوراً از اطلاعات خود بک‌آپ تهیه کنید و آن را در جایی خارج از کامپیوتر خود، مثلاً یک هارد اکسترنال، نگاه دارید که در این صورت حتی اگر مورد حملهٔ هکرها قرار گیرید، تاحدی آرامش دارید چرا که خیالتان راحت است که نسخه‌ای از اطلاعات خود را در اختیار دارید. نکتهٔ دیگری که باید مدنظر داشته باشید این است که از باز کردن فایل‌های پیوست شده (Attachments) به ایمیل‌های ناشناس جداً خودداری کنید. علاوه بر این، لازم است سیستم‌عامل خود را به‌روز کنید تا به این ترتیب در مقابل یک حملهٔ احتمالی قریب‌الوقوع آماده‌تر باشید.

لازم به ذکر است که مایکروسافت به منظور رفع اشکالات ویندوز XP که مورد استفادهٔ این باج‌افزار قرار گرفته، اقداماتی را انجام داد اما همیشه این اتفاق نمی‌افتد و شرکت‌های نرم‌افزاری نمی‌توانند هر زمانی که محصول قدیمی آن‌ها مورد حمله قرار گرفت، شروع به انتشار آپدیت‌های امنیتی کنند. یکی از دلایل موفقیت‌آمیز بودن این حمله‌ها نیز همین بی‌توجهی کاربران نسبت به استفاده از محصولات و آپدیت‌های جدید است؛ به هر حال اگر شما به فکر امنیت خود نباشید، شرکت‌های نرم‌افزاری نمی‌توانند کار زیادی برای امنیت شما انجام دهند.

آیا اگر دچار حمله قرار گرفتیم می‌بایست باج دهیم؟

هرچند معمولاً در همهٔ کامپیوترها اطلاعات حساس و مهمی پیدا می‌شود، اما پاسخ این سؤال کاملاً به نوع و اهمیت داده‌های شما بستگی دارد. در هر صورت، اگر مورد حملهٔ این باج‌افزار قرار گرفتید، لازم است که تصمیم بزرگی بگیرید و به طور کلی دو راه پیش‌روی شما قرار دارد:

- راه اول اینکه مبلغ خواسته شده را به هکرها پرداخت نموده و به فایل‌های خود دسترسی پیدا کنید و از طرفی آن‌ها را در ادامه دادن به این راه شیطانی تشویق نمایید!

- راه دوم اینکه همهٔ اطلاعات رمزنگاری شده را پاک کنید و همه‌چیز را از صفر شروع کنید!

طبیعتاً راه دوم دشوارتر است. از سوی دیگر، انتخاب این راه در برخی موارد غیرممکن نیز هست. مثلاً برای شرکت‌هایی که کل سیستم‌های خود را به صورت یک شبکهٔ واحد سازماندهی درآورده‌اند، صرف‌نظر کردن از کل اطلاعات غیرممکن به نظر می‌رسد. از سوی دیگر، مبلغی که هکرها در ابتدا درخواست می‌کنند در مقایسه با دارایی این شرکت‌ها ناچیز است و طبیعتاً شرکت‌ها ترجیح می‌دهند به جای از دست دادن اطلاعات ارزشمند خود، اندکی از دارایی خود را از دست بدهند (البته در برخی موارد نیز شاهد هستیم که هکرها پس از دریافت مبلغ اولیه، مجدداً مبالغ بیشتر و بیشتری را درخواست نموده‌اند.) هر چند ممکن است گاهی چاره‌ای جز پرداخت مبالغ خواسته شده وجود نداشته باشد، اما به هر حال باج دادن یک انتخاب ایده‌آل نیست.

سخن آخر اینکه همواره از اطلاعات مهم خود بک‌آپ بگیرید زیرا نمی‌دانید چه زمانی دچار مشکل خواهید شد؛ شاید همین الان، شاید لحظه‌ای بعد و شاید روزی دیگر.

حمله باج‌افزار واناکرای

حملهٔ باج‌افزار واناکرای (به انگلیسی: WannaCry) که یک حمله سایبری جهانی بود به نام‌های WannaCrypt یا WanaCrypt0r 2.0 نیز شناخته می‌شود، ابزاری برای اجرای حملات باج‌افزاری است. در ماه می سال ۲۰۱۷ میلادی، حمله سایبری عظیمی با استفاده از این باج‌افزار آغاز شد که بیش از ۲۳۰ هزار رایانه را در ۱۵۰ کشور جهان را آلوده ساخت و به ۲۸ زبان از قربانیان باج طلب می‌کند. حمله مذکور آن گونه که یوروپول توصیف کرده‌است، بی‌سابقه بوده‌است.

این حمله سایبری، چند شرکت در اسپانیا مانند تلفونیکا و همچنین «سازمان ملی تأمین بهداشت و درمان» (NHS) بریتانیا، فدکس و دویچه بان را تحت تأثیر قرار داد. اهداف دیگر نیز در حدود ۱۵۰ کشور همزمان گزارش شده‌اند. بالغ بر یک هزار رایانه در وزارت کشور، وزارت بحران و شرکت مخابراتی مگافون روسیه نیز گزارشی مبنی بر آلودگی داده‌اند.

محققان امنیت سایبری مدارکی را دال بر این موضوع کشف کرده‌اند که ممکن است کره شمالی با حمله بین‌المللی واناکرای به عنوان باج افزار در ارتباط باشد. این حمله سایبری در این ماه ۳۰۰٬۰۰۰ رایانه در ۱۵۰ کشور دنیا را مبتلا کرده‌است. دولت پیونگ‌یانگ چنین ادعایی را «مسخره» خوانده‌است. هکرهای اجراکننده این باج‌افزار، در ازای دریافت رمزارز بیت‌کوین اقدام به آزادسازی فایل‌های رمزگذاری‌شده می‌نمودند که همین موضوع، ردیابی آنها را با دشواری مواجه می‌نمود.

پیش‌زمینه

باج‌افزار واناکرای از اکسپلویت اترنال بلو استفاده کرده‌است که توسط آژانس امنیت ملی ایالات متحده آمریکا برای حمله رایانه‌های دارای سیستم‌عامل مایکروسافت ویندوز نوشته شد. وجود اترنال بلو، نخستین‌بار توسط گروه رخنه‌گر «The Shadow Brokers» در ۸ آوریل ۲۰۱۷ مشخص شد. اترنال بلو در میان ابزارهای دیگر لو رفته از اکوئیشن گروپ در ۱۴ آوریل ۲۰۱۷ منتشر شد. مشخص شده که اکوئیشن گروپ جزئی از آژانس امنیت ملی آمریکا است.

اترنال بلو از آسیب‌پذیری MS17-010 در پیاده‌سازی بلوک پیام سرور سوء استفاده می‌کند. مایکروسافت توصیه‌ای بحرانی به همراه یک وصله امنیتی برای رفع آسیب‌پذیری در ۱۴ مارس ۲۰۱۷ منتشر کرد. اما این وصله فقط ویندوز ویستا و سیستم‌عامل‌های پس از آن، به جز ویندوز اکس‌پی را تعمیر نمود.

هرچند وصله نرم‌افزاری MS17-010 برای حذف اساسی آسیب‌پذیری در ۱۴ مارس ۲۰۱۷ منتشر شده بود اما تأخیر در اعمال بروزرسانی‌های امنیتی، برخی کاربران و سازمان‌ها را آسیب‌پذیر باقی گذاشت. توجه شود که ویندوز ۱۰ از این حمله مصون است.

عملکرد

در تاریخ ۱۲ می ۲۰۱۷، باج‌افزار WannaCry آلوده‌سازی رایانه‌های سراسر جهان را آغاز کرد. این باج‌افزار پس از دستیابی به رایانه‌ها، درایو دیسک سخت این رایانه‌ها را رمزگذاری می‌کند و سپس برای سوء استفاده

از آسیب‌پذیری SMB برای انتشار به صورت تصادفی در رایانه‌های متصل به اینترنت و همچنین بین رایانه‌های روی شبکه محلی تلاش می‌کند.

تأثیر

اقدامات تهاجمی این باج‌افزار بر اساس اعلام یوروپول بی‌سابقه بوده‌است. این حمله بسیاری از بیمارستان‌های خدمات بهداشتی ملی بریتانیا را تحت تأثیر قرار داده‌است. در تاریخ ۱۲ می ۲۰۱۷، برخی خدمات این سازمان از موارد اورژانسی غیر بحرانی دور شدند و چند آمبولانس به جای اشتباهی ارسال شدند. هزاران رایانه سازمان ملی تأمین بهداشت و درمان بریتانیا که همچنان از ویندوز اکس‌پی استفاده می‌کنند ۴۲ سرویس موقعیت‌یاب را اشتباه گزارش داده‌اند. شرکت خودروسازی نیسان موتورز در تاین و ور، یکی از کارخانه‌های بزرگ خودروسازی، تولید خود را پس از آلوده شدن توسط این باج‌افزار متوقف کرد. شرکت خودروسازی رنو نیز تولیدات خود را در چند کارخانه خود در تلاش برای متوقف‌سازی این باج‌افزار متوقف نمود.

فهرستی از شرکت‌ها و موسسات آلوده شده

- سازمان ملی تأمین بهداشت و درمان (NHS) بریتانیا
- ایستگاه راه‌آهن در شهر فرانکفورت آلمان
- دانشگاه میلانو-بیکوکا در ایتالیا
- بانکو بیلبائو ویسکایا آرخنتاریا
- خودروسازی نیسان
- کتابخانه در عمان
- خودروسازی رنو
- مگافون روسیه
- دویچه بان
- تلفونیکا
- فدکس
- بانک سپه ایران

کلید قطع اضطراری

چند ساعت پس از انتشار اولیه این باج‌افزار در ۱۲ می ۲۰۱۷، یک «کلید قطع اضطراری» تصریح شده در داخل بدافزار کشف شد. این کلید امکان داد که با ثبت یک دامنه اینترنتی گسترش اولیه آلودگی متوقف شود.

این کلید قطع اضطراری به یک کدنویسی اشتباه در مجموعه مجرمان تظاهر می‌نمود و انتظار می‌رفت گونه‌ها بدون این کلید قطع اضطراری ساخته شوند.

وصله امنیتی

این آسیب‌پذیری ویندوز از نوع آسیب‌پذیری حمله روز صفر نیست. اما در ۱۴ مارس ۲۰۱۷ مایکروسافت یک وصله امنیتی به نام MS17-010 را برای تمام نسخه‌هایی که مورد حمله باج‌افزار WannaCry قرار گرفته‌اند از جمله ویندوز اکس‌پی، ویندوز سرور ۲۰۰۳ و ویندوز ۸ ارائه داد.

این وصله برای پروتکل بلوک پیام سرور SMB مورد استفاده ویندوز بود. مایکروسافت همچنین توصیه می‌کند که کاربران استفاده از پروتکل قدیمی SMB1 را متوقف کرده و به جای آن از SMB3 که جدیدتر و امن‌تر است استفاده کنند. سازمان‌هایی که این وصله امنیتی را ندارند به همین دلیل آلوده شدند. هرچند تابحال مدرکی دربارهٔ حمله خاص برنامه نویسان این باج‌افزار به این سازمان‌ها وجود نداشته‌است. هر سازمانی که همچنان از ویندوز اکس‌پی که به پایان عمر رسیده‌است استفاده می‌کند در معرض خطر بسیار زیادی است.

پیشگیری

- ساده‌ترین راه جهت پیشگیری از آلوده شدن رایانه، نصب وصله امنیتی MS17-010 برای همه نسخه‌های ویندوز است.
- سیستم‌عامل و ضدویروس و رایانه خود را به‌روز نگه دارید.
- درصورت امکان از ویندوزهای ایکس‌پی، سرور ۲۰۰۰ و سرور ۳۰۰۰ استفاده نکنید.
- پورت‌های ۱۳۹/۴۴۵ و ۳۳۸۹ را روی دیوار آتش مسدود کنید.
- به‌طور منظم از فایل‌های خود، نسخه پشتیبان تهیه کنید.

پس از آلودگی

- به محض آلوده شدن، کامپیوتر خود را از شبکه خارج کنید تا از تکثیر این کِرم جلوگیری شود.
- هرگز پول باج‌خواهی شده را پرداخت نکنید زیرا احتمال بازگشت اطلاعات قفل شده حتی پس از طریق پرداخت باج تقریباً غیرممکن است.
- با توجه به شدت آلودگی، احتمالاً بهترین روش پاکسازی، نصب دوباره ویندوز است.
- تاکنون راهی برای بازیافت اطلاعات رمزگذاری شده توسط باج‌افزار پیدا نشده‌است. اما چون احتمال کد آزادسازی پرونده‌های قفل شده در آینده وجود دارد، پیش از شروع عملیات پاکسازی، از اطلاعات خود نسخه پشتیبان تهیه کنید.

واکنش‌ها

- پس از آگاهی از تأثیر این حمله سایبری بر خدمات بهداشتی ملی بریتانیا، ادوارد اسنودن گفت اگر آژانس امنیت ملی آمریکا نقص مورد استفاده برای حمله به بیمارستان‌ها را به عنوان قانون افشای مسئولانه در زمان یافتن آن و نه در هنگام از دست دادن آن در اختیار داشت، این حمله باج‌افزاری امکان داشت رخ ندهد.
- ترزا می، نخست‌وزیر بریتانیا دربارهٔ این باج‌افزار گفت این باج‌افزار فقط خدمات بهداشتی ملی بریتانیا را هدف نگرفته‌است. این یک حمله بین‌المللی است. تعدادی کشور و سازمان آلوده شده‌اند.
- مایکروسافت وصله‌های امنیتی را برای ورژن‌های جدید ویندوز از جمله ویندوز اکس‌پی، ویندوز ۸ و ویندوز سرور ۲۰۰۳ که پشتیان نمی‌شوند، ایجاد کرد.

در ایران

بر اساس آماری که سازمان فناوری اطلاعات ایران در اواخر اردیبهشت ۱۳۹۶ منتشر کرد باج‌افزار واناکرای بیش از ۲ هزار قربانی در ایران داشته که در این میان استان‌های اصفهان و تهران بیشترین تعداد قربانی را داشته‌اند.

باج افزار WannaCry

باج گیری الکترونیکی ، دیگر این روزها تبدیل به یک روش متداول برای هکر ها و افراد مخرب شده است. با رشد چشمگیر ارز های الکترونیکی ، از جمله بیتکوین (BitCoin) و سادگی انتقال وجه بدون رهگیری گیرنده آن ، هر روزه شاهد رشد قابل توجه این نوع حملات هستیم، به طوری که بنظر می رسد باج افزار در حال تبدیل شدن به روش شماره یک هکر ها در آلوده کردن سیستم ها می باشد. باج‌افزارها (Ransomware) گونه‌ای از بدافزارها هستند.

رمز گذاری اطلاعات

استفاده از انواع روش های رمزگذاری دسترسی به سیستم را محدود می‌کند و شخص نفوذ کننده یا هکر در ازای دریافت وجه، امکان مجدد بازیابی فایل ها را برای قربانی فراهم می آورد. برخی از انواع باج افزارها روی فایل‌های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام‌هایی روی نمایشگر نشان دهند که از کاربر می‌خواهد برای رفع آن مبالغی را به حساب آنها واریز کنند.

طی روزهای اخیر باج افزاری با نام واناکرای (WannaCry) که به صورت خلاصه WCry نامیده می شود بالغ بر ۲۳۰ هزار رایانه را در ۹۹ کشور آلوده ساخته است . حمله‌ی این بدافزار از روز جمعه آغاز شده و گفته می‌شود خطرناک‌ترین باج‌افزاری است که تاکنون مشاهده شده است. این باج‌افزار صنایع و نهادهای مختلفی را در کشورهای متعدد از جمله بیمارستان‌های انگلستان، شرکت‌های مخابراتی اسپانیا، بانک‌های روسیه و تولیدکنندگان ماشین در اروپا را هدف حمله‌ی خود قرار داده است.

بد افزار WannaCry

بدافزار WannaCry از آسیب‌پذیری با شناسه‌ی MS۱۷-۰۱۰ بهره برداری می‌کند که بر روی بسیاری از نسخه‌های سیستم عامل ویندوز این آسیب‌پذیری وجود دارد. این آسیب‌پذیری زمانی به‌طور عمومی افشاء شد که یک گروه نفوذ با نام Shadow Brokers، ابزارهای نفوذ متعلق به آژانس امنیت ملی آمریکا را به‌طور آنلاین منتشر کردند.

باج‌افزار WannaCry یک بدافزار ترکیبی است که در مرحله‌ی توزیع، رفتاری شبیه به یک کرم دارد، این ویژگی توزیع، باعث شده WannaCry خطرناک‌ترین باج‌افزاری باشد که تاکنون ظاهر شده است. برای اینکه خود را از این حملات در امان نگه دارید، چندین راه‌حل وجود دارد. یکی از این راه‌حل‌ها این است که از نسخه‌های به‌روزرسانی‌شده‌ی ویندوز استفاده کنید. در حال حاضر شرکت مایکروسافت برای برطرف کردن این آسیب‌پذیری وصله‌هایی را منتشر کرده است.

این باج‌افزار به زبان CPP نوشته شده بود که هیچ تلاشی نیز برای مخفی بودن کد اصلی در آن مشاهده نشد. همانند بسیاری از خانواده‌ی باج‌افزارها، WCry در فرآیند رمزگذاری پس از تعویض نام فایل‌ها و فرمت آن را نیز به WNCRY. تغییر می‌دهد. پس از آلوده شدن سیستم، صفحه‌ای باج خواهانه، مبنی‌بر پرداخت بیت‌کوین به ارزش 300 دلار را نمایش داده می شود.

چه ویندوزهایی تحت تاثیر این باج افزار WCry قرار دارند؟

همه‌ی نسخه‌های سامانه‌عامل ویندوز، از جمله ویندوز اِکس‌پی، ویندوز ویستا، ویندوز سِون، ویندوز ۸ و ویندوز ۱۰ و همه‌ی نسخه‌های کارگزار ویندوز (Windows Server) تحت تأثیر هستند. - مایکروسافت به‌روزرسانی‌هایی را برای همه‌ی نسخه‌های ویندوز (به جز ویندوز اِکس‌پی) دو ماه پیش منتشر کرده است. و در روز گذشته به‌روزرسانی فوری برای ویندوز اِکس‌پی منتشر شده است (گفتنی است ویندوز اِکس‌پی توسط مایکروسافت پشتیبانی نمی‌شود اما به دلیل اهمیت و گستردگی انتشار باج‌افزار WannaCry، به‌روزرسانی فوری برای این نسخه از ویندوز منتشر شده است)

چگونه با باج افزار WCry مقابله کنیم؟

اگر شما از فایروال استفاده می‌کنید باید پورت شماره‌ی ۴۴۵ را مسدود نمایید. این پورت برای ارتباطات نرم‌افزار SMB استفاده می‌شود و راه جلوگیری ا انتشار این باج‌افزار مسدود نمودن پورت مورد نظر می‌باشد. البته برای این کار از فایروال ویندوز نیز می‌توانید استفاده کنید. کافی است به مسیر System and Security در کنترل پنِل وارد شوید و سپس Windows Firewall را انتخاب نمایید. از ستون سمت چپ گزینه‌ی Advanced settings را انتخاب کنید. سپس برای مشاهده‌ی قوانین دیواره‌ی آتش بخش Inbound Rules را باز نمایید. سپس از منوی سمت راست گزینه‌ی New Rule را انتخاب کرده و با انتخاب نوع Port، پورت ۴۴۵ , ۱۳۷ و ۱۳۹ در پروتکل TCP و پورت ۱۳۷ و ۱۳۸ UDP را مسدود نمایید. پس از ایجاد رول مورد نظر با راست کلیک روی آن، رول را فعال نمایید.

همچنین از طریق راهنمای ذیل می توانید اقدام به غیر فعال نمودن سرویس SMB نمایید.

بر روی Windows 7 و windows Server 2008 می بایست دو دستور زیر را در CMD اجرا نمائید و پس از آن ویندوز را ریستارت نمائید:

sc config lanmanworkstation depend= bowser/mrxsmb20/nsi

sc config mrxsmb10 start= disabled

بر روی ویندوز 10 و همچنین ویندوز سرور 2012 و 2016 می بایست feature با عنوان SMB 1.0/CIFS File Sharing Support را از windows feature حذف نمائید.

و برای ویندوز سرور ۲۰۰۳ و موارد دیگر می بایست از پکیج های موجود در لینک زیر استفاده فرمائید:

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

در آخر این نکته را نیز در نظر داشته باشید که حتما آخرین بسته های به روز رسانی سیستم عامل خود را نصب نمایید.

حمله سایبری نسخه دوم باج افزار WannaCry (نسخه اولیه اولین بار در مارس 2017 ظاهر شد) در ماه می سال ۲۰۱۷ آغاز و در ابتدا 125000 رایانه متصل به اینترنت را آلوده کرد.

این نسخه بسیار مخرب از باج افزار از جفت آسیب پذیری های zero-day -روز صفرم (ETERNALBLUE و DOUBLEPULSAR) که برای اولین بار توسط NSA شناسایی و توسط یک گروه هک معروف به نام " The Shadow Brokers" فاش شد، سوء استفاده می کنند. آسیب پذیری های عنوان شده از نقاط ضعف SMB (DOUBLEPULSAR) و همچنین از خواص شبیه کرم (ETERNALBLUE) استفاده می کنند.

رفتار کرم مانند به این معنی است که باج افزار از یک سیستم به سیستم دیگر ، بدون دخالت کاربر و به طور خودکار به هر مخاطب قربانی که می تواند پیدا کند، گسترش می یابد.

WannaCry ، مانند اکثر باج افزارها، با رمزگذاری فایل های شما و درخواست پرداخت باج برای مبادله کلید رمزگشایی فایل هایتان، عمل می کند. باج دادن از 300 دلار برای 6 ساعت اول شروع می شود ، قربانی تا 3 روز برای پرداخت باج قبل از دو برابر شدن به 600 دلار فرصت دارد. اگر تا یک هفته پرداخت نکنید، پس از آن طراح باج افزار تهدید می کند که فایل ها را با هم حذف می کند. WannaCry حتی به قربانی اجازه می دهد تا تعداد کمی فایل را رمزگشایی کند تا نشان دهد که در واقع فایل های خود را پس خواهید گرفت.

WannaCry چگونه انتقال داده می شود؟

توزیع اولیه WannaCry از طریق ایمیل فیشینگ گسترش پیدا کرد. WannaCry در یک فایل zip. محافظت شده با رمز عبور پنهان شد (رمز عبور به منظور نمایش امنیت بیش تر در ایمیل گنجانده شده بود) که پس از اجرای پرونده zip. باج افزار اجرا می شود.

این باج افزار با بهره برداری از ETERNALBLUE zero-day خصوصیاتی کرم مانندی را با اسکن پورت باز 445 جهت دسترسی به پروتکل SMB(سرویس اشتراک‌گذاری فایل‌ها) از خود نشان می دهد. این یک روال رمزگذاری را آغاز کرده و نه تنها میزبانان شبکه محلی بلکه میزبان های موجود در اینترنت نیز آلوده می شوند.

چگونه می توان در برابر WannaCry از اطلاعات خود محافظت کرد؟

- اگر هنوز این کار را نکرده اید ، حتماً به روزرسانی امنیتی MS17-010 مایکروسافت را نصب کنید ، که در وهله اول مانع از تأثیرگذاری WannaCry در سیستم عامل ویندوز شما می شود.
- فایروال را فعال کنید و پورت‌های) SMB بر روی پورت‌های TCP شامل ۱۳۷، ۱۳۹ و ۴۴۵ و بر روی پورت‌های UDP شامل ۱۳۷ و ۱۳۸) را مسدود کنید.
- اگر سازمان شما از Windows Defender استفاده می کند ، می توانید تعاریف تهدید به روز شده را دانلود کنید که به شما امکان می دهد WannaCry را در یک میزبان تشخیص دهید:

https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt

اگر فایل های شما قبلاً رمزگذاری شده اند، می توانید لیستی از گزینه های بازیابی و حذف بدافزارها را در اینجا بیابید:

/http://www.besttechtips.org/remove-wannacry-ransomware-decrypt-wncry-files

- اگر سعی کردید که از نسخه پشتیبان تهیه شده خود استفاده کنید ولی شکست خورده اید (یا در مرحله اول نسخه های پشتیبان ندارید)، برنامه ای مانند Shadow Explorer را امتحان کنید تا ببینید که آیا این باج افزار کپی های Shadow Volume شمارا حذف نکرده است. اگر کاربر در UACروی بله کلیک نکرد ، هنوز شانسی برای شروع بازیابی وجود دارد.
- به عنوان آخرین راه حل اگر بازیابی فایل ها و پشتیبان گیری با موفقیت انجام نشد، می توانید فایل های خود را با پرداخت مبلغی بازیابی و رمزگشایی کنید.

یکی از ساده ترین راه های نظارت بر اتفاقاتی که در شبکه شما رخ می دهد ، تنظیم پورت SPAN \ Mirror یا استفاده از یک network TAP است. این امر به شما امکان دسترسی به جریان ها و بارهای بسته را می دهد ، بنابراین می توانید ببینید چه کسی به چه چیزی وصل می شود و چه موارد مشکوکی در اطراف وجود دارد

نظارت چهار چیز برای تشخیص WannaCry

1. بررسی استفاده از SMBv1
2. بررسی افزایش نرخ تغییر نام فایل در شبکه خود
3. بررسی موارد @Please_Read_Me@.txt روی فایل های اشتراکی
4. بررسی هر گونه فایل با این پسوندها:

- **.wnry**
- **.wcry**
- **.wncry**
- **.wncryt**

WannaCry نمونه ای از باج افزار رمزنگاری است، نوعی نرم افزار مخرب (بدافزار) که توسط مجرمان سایبری برای اخاذی پول استفاده می شود.

باج افزار این کار را با رمزگذاری پرونده های با ارزش انجام می دهد، بنابراین شما قادر به خواندن آنها نیستید یا با قفل کردن کامپیوتر خود، نمی توانید از آنها استفاده کنید. باج افزاری که از رمزگذاری استفاده می کند باج افزار رمزنگاری نامیده می شود. به نوعی که شما را از کامپیوتر قفل می کن ، باج افزار Locker گفته می شود.

مانند انواع دیگر باج افزارهای رمزنگاری، WannaCry داده های شما را به گروگان می گیرد و قول می دهد در صورت پرداخت باج، آنها را بازگرداند.

WannaCry رایانه های که از Microsoft Windows استفاده می کنند به عنوان یک سیستم عامل هدف قرار می دهد. این داده ها را رمزگذاری می کند و برای بازپرداخت آن درخواست باج توسط ارز رمزنگاری شده بیت کوین را دارد. حمله باج افزار WannaCry یک اپیدمی جهانی بود که در ماه مه سال 2017 اتفاق افتاد.

حمله WannaCry چگونه کار می کند؟

مجرمان سایبری مسئول این حمله، از ضعف سیستم عامل Microsoft Windows با استفاده از هک استفاده کردند که گفته می شود توسط آژانس امنیت ملی ایالات متحده توسعه یافته است. این هک که به عنوان EternalBlue شناخته می شود، توسط گروهی از هکرها به نام Shadow Brokers قبل از حمله WannaCry علنی شد.

مایکروسافت تقریباً دو ماه قبل از شروع حمله باج افزار WannaCry، یک وصله امنیتی منتشر کرد که سیستم های کاربر را در برابر این بهره برداری محافظت می کرد. متأسفانه، بسیاری از افراد و سازمان ها به طور منظم سیستم عامل خود را به روز نمی کنند و بنابراین در معرض حمله قرار می گیرند.

کسانی که قبل از حمله به روزرسانی مایکروسافت ویندوز را اجرا نکرده بودند از وصله استفاده نکردند و آسیب پذیری مورد استفاده توسط EternalBlue آنها را برای حمله باز گذاشت.

هنگامی که این اتفاق برای اولین بار رخ داد، مردم تصور می کردند که حمله باج افزار WannaCry در ابتدا از طریق یک کمپین فیشینگ گسترش یافته است (یک کمپین فیشینگ جایی است که ایمیل های هرزنامه با پیوندها یا پیوست های آلوده کاربران را به بارگیری بدافزار سوق می دهد). با این حال، EternalBlue سوء استفاده ای بود که به WannaCry امکان انتشار و گسترش را می دهد.

اگر باج WannaCry پرداخت نشود چه اتفاق افتاد؟

مهاجمان خواستار بیت کوین به ارزش 300 دلار بودند و بعداً تقاضای باج را به 600 دلار بیت کوین افزایش دادند. اگر قربانیان ظرف سه روز باج را پرداخت نکنند، به قربانیان حمله باج افزار WannaCry گفته شد که پرونده های آنها برای همیشه پاک می شود.

توصیه در مورد پرداخت باج این است که تحت تاثیر فشار قرار نگیرید. همیشه از پرداخت باج بپرهیزید، زیرا هیچ تضمینی وجود ندارد که داده های شما پس داده شود.

این توصیه در طول حمله WannaCry عاقلانه به نظر می رسید زیرا، طبق گزارشات، کدگذاری مورد استفاده در حمله معیوب بود. وقتی قربانیان باج خود را پرداخت می کردند، مهاجمان به هیچ وجه نمی توانستند پرداخت را با رایانه قربانی خاصی مرتبط کنند.

در مورد اینکه کسی پرونده های خود را پس گرفته است یا نه شک دارد. برخی از محققان ادعا کردند که هیچ کس اطلاعات خود را پس نمی گیرد. با این حال شرکتی به نام F-Secure ادعا کرد که برخی این کار را کردند. این یک یادآوری جدی برای این است که اگر حمله به باج افزار را تجربه می کنید، هرگز فکر خوبی نیست که باج را بپردازید.

حمله WannaCry چه تاثیری داشت؟

حمله باج افزار WannaCry حدود 230،000 رایانه در سطح جهان را تحت تأثیر قرار داد. یکی از اولین شرکت هایی که تحت تأثیر قرار گرفت شرکت تلفن همراه اسپانیایی، Telefónica بود. تا 12 ماه مه، هزاران بیمارستان و جراحی NHS در سراسر انگلیس تحت تأثیر قرار گرفتند.

یک سوم اعتماد بیمارستان NHS تحت تأثیر این حمله قرار گرفت. گفته می شود که آمبولانس ها به طرز وحشتناکی تغییر مسیر داده و افرادی را که نیاز به مراقبت فوری دارند نیاز دارند. پس از لغو 19000 قرار ملاقات در نتیجه حمله، هزینه NHS هنگفت 92 میلیون پوند تخمین زده شد.

با گسترش باج افزار به خارج از اروپا، سیستم های رایانه ای در 150 کشور جهان فلج شدند. حمله باج افزار WannaCry تأثیر مالی قابل توجهی در سراسر جهان داشت. تخمین زده شده است که این جرایم اینترنتی موجب خسارت 4 میلیارد دلاری در سراسر جهان شده است.

محافظت در برابر باج افزار

اکنون می فهمید که چگونه حمله باج افزار WannaCry رخ داده و تاثیری که بر آن وارد شده است، بیایید بررسی کنیم که چگونه می توانید خود را در برابر باج افزار محافظت کنید.

در اینجا نکات برتر ما وجود دارد:

1. نرم افزار و سیستم عامل خود را مرتباً به روز کنید.

کاربران رایانه قربانی حمله WannaCry شدند زیرا آنها سیستم عامل Microsoft Windowsخود را بروزرسانی نکرده بودند.

اگر آنها سیستم عامل خود را مرتباً به روز می کردند، از وصله امنیتی مایکروسافت که قبل از حمله منتشر شده بود، بهره مند می شدند.

این پچ آسیب پذیری که توسط EternalBlue برای آلوده کردن رایانه ها به باج افزار WannaCryمورد سو استفاده قرار گرفت، از بین رفت.

حتماً نرم افزار و سیستم عامل خود را به روز کنید. این یک مرحله ضروری برای محافظت از باج افزار است.

2. روی پیوندهای مشکوک کلیک نکنید.
اگر ایمیل ناآشنایی را باز کردید یا از وب سایتی بازدید کردید، اعتماد ندارید، روی هیچ پیوندی کلیک نکنید. با کلیک بر روی پیوندهای تأیید نشده می توانید باج افزار را بارگیری کنید.

3. هرگز پیوست های ایمیل نامعتبر را باز نکنید.
از اطمینان از ایمن بودن ضمیمه نامه های ایمیل خودداری کنید. آیا شما فرستنده را می شناسید و به او اعتماد دارید؟ آیا مشخص است که پیوست چیست؟ آیا انتظار داشتید پرونده پیوست را دریافت کنید؟
اگر پیوست از شما خواسته است که ماکروها را برای مشاهده آن فعال کنید، کاملاً محتاط باشید. ماکروها را فعال یا پیوست را باز نکنید زیرا این یک روش رایج برای باج افزار و انواع دیگر بدافزارها است.

4. از وب سایت های نامعتبر بارگیری نکنید.
بارگیری پرونده ها از سایت های ناشناخته خطر بارگیری باج افزار را افزایش می دهد. فقط پرونده ها را از وب سایت های مورد اعتماد خود بارگیری کنید.

5. از USB های ناشناخته خودداری کنید.
اگر نمی دانید آنها از کجا آمده اند، USB یا سایر دستگاه های ذخیره سازی حذف را وارد رایانه نکنید. آنها می توانند به باج افزار آلوده شوند.

6. هنگام استفاده از Wi-Fi عمومی از VPN استفاده کنید.
هنگام استفاده از Wi-Fi عمومی احتیاط کنید زیرا این باعث می شود سیستم رایانه شما در برابر حمله آسیب پذیرتر شود.
برای محافظت در برابر خطر بدافزار هنگام استفاده از Wi-Fi عمومی از VPN امن استفاده کنید.

7. نرم افزار امنیت اینترنتی را نصب کنید.
با نصب نرم افزار امنیت اینترنتی از رایانه خود محافظت کرده و از باج افزار جلوگیری کنید. به دنبال یک راه حل جامع باشید که از چندین تهدید پیچیده محافظت کند، مانند Kaspersky's System Watcher.

8. نرم افزار امنیت اینترنت خود را به روز کنید.
برای اطمینان از دریافت حداکثر حفاظت، امنیت اینترنت شما (شامل همه جدیدترین وصله ها) به روز نگه دارید.

9. از اطلاعات خود پشتیبان تهیه کنید.

حتماً با استفاده از یک هارد اکسترنال یا فضای ذخیره سازی ابری به طور منظم از اطلاعات خود پشتیبان تهیه کنید. اگر قربانی هکرهای باج افزار شوید، در صورت تهیه نسخه پشتیبان از اطلاعات شما ایمن خواهد بود. فقط به یاد داشته باشید که پس از پشتیبان گیری از اطلاعات خود، دستگاه ذخیره سازی خارجی خود را با رایانه جدا کنید. ثابت نگه داشتن فضای ذخیره سازی خارجی با رایانه به طور بالقوه آن را در معرض خانواده های باج افزار قرار می دهد که می توانند داده های این دستگاه ها را نیز رمزگذاری کنند.

اترنال بلو

اترنال‌بلو یک اکسپلویت است که عموماً توسط آژانس امنیت ملی ایالات متحده آمریکا توسعه یافته‌است. این اطلاعات توسط شادو بروکرز (گروه هکری شکنندگان سایه) در ۱۴ آوریل ۲۰۱۷ افشا شد و به عنوان بخشی از حمله جهانی باج افزار واناکرای در ۱۲ می۲۰۱۷ مورد استفاده قرار گرفت.

جزئیات

اکسپلویت اترنال‌بلو یک آسیب‌پذیری در پروتکل بلوک پیام سرور از مایکروسافت است. این آسیب‌پذیری در کاتالوگ آسیب‌پذیری‌های رایج و افشا شده با ورودی CVE-2017-0144 نشان داده می‌شود. این آسیب‌پذیری وجود دارد به دلیل اینکه بلوک پیام سرور نسخه یک سروری در نسخه‌های مختلف ویندوز پاکت طراحی شده توسط حمله کننده از راه دور را می‌پذیرد؛ و به آنها اجازه می‌دهد کدهای دلخواهشان را بر روی کامپیوتر هدف اجرا کنند.

در ۱۴ مارس ۲۰۱۷ بولتن امنیتی را با نام MS17-010 را منتشر کرد، که نقص دقیق را اعلام می‌کرد و در آن نسبت به وصله‌های امنیتی که برای تمامی نسخه‌های ویندوز که در آن زمان مورد پشتیبانی قرار می‌گرفتند اطلاع می‌رسانی می‌کرد. وصله‌های امنیتی برای این ویندوزها که شامل ویندوز ۷، ویندوز ۸/۱، ویندوز ۱۰، ویندوز سرور ۲۰۰۸، ویندوز سرور ۲۰۱۲ و ویندوز سرور ۲۰۱۶ و همچنین برای ویندوز ویستا با وجود پایان پشتیبانی آن فراهم شده بود. بسیاری از کاربران این وصله‌های امنیتی را نصب نکرده بودند. تا اینکه در دو ماه بعد در ۱۲ مه ۲۰۱۷ حمله باج افزار واناکرای با استفاده از آسیب‌پذیری اترنال‌بلو انجام شد و خودش را گسترش داد. روز بعد مایکروسافت وصله‌های امنیتی اورژانسی را برای ویندوزهای ویندوزاکس‌پی، ویندوز سرور ۲۰۰۳ و ویندوز ۸ که توسط این شرکت پشتیبانی نمی‌شدند را منتشر کرد.

روش مقابله با اکسپلویت EternalBlue (CVE-2017-0146 / MS17-010)

مقدمه

در سال ۲۰۱۷ میلادی یک آسیب‌پذیری حیاتی به نام EternalBlue در سیستم عامل ویندوز میکروسافت به صورت عمومی افشا گردید که به نفوذگر اجازه می‌داد از راه دور و با برقراری ارتباط روی پورت ۴۴۵ (SMB) روی سیستم آسیب‌پذیر کد دلخواه خود را اجرا نماید. این آسیب‌پذیری که تا پیش از آن، سال‌ها مورد استفاده سازمان‌های جاسوسی آمریکایی بود به صورت عمومی افشا شده و کد استفاده از آن در اختیار بدافزارنویسان قرار گرفت.

اگر چه میکروسافت همان موقع اقدام به انتشار وصله جهت نسخه‌های آسیب‌پذیر ویندوز نمود و حتی بعد از مدتی برای ویندوزهای XP و ۲۰۰۳ که منسوخ محسوب می‌شدند نیز وصله‌های خارج از نوبت ارائه کرد؛ اما به علت در دسترس بودن کد حمله و نصب نکردن وصله توسط بسیاری از کاربران، همچنان شاهد حملات گسترده از طریق این آسیب‌پذیری هستیم و بسیاری از بدافزارها و کرم‌های شبکه نیز از این روش برای انتشار خود استفاده می‌کنند.

راهکارها و توصیه‌ها

در ادامه به موارد زیر پرداخته خواهد شد:

1. چگونه سیستم / شبکه خود را برای آسیب‌پذیر بودن تست نماییم؟
2. راهکارهای اصلی رفع آسیب‌پذیری
3. راهکارهای موقت و جایگزین
4. راهکارهای کاهش ریسک در شبکه

تست آسیب‌پذیری – آیا سیستم من آسیب‌پذیر است؟

روش تست یک سیستم

جهت تست آسیب‌پذیری سیستم می‌توانید از اسکریپت زیر استفاده نمایید:

1. اسکریپت check-eternalblue.ps1 را دانلود نمایید. (این اسکریپت توسط میکروسافت تهیه شده است)
2. پس از اجرا، پیام سبز رنگ «System is Patched» نشانگر این است که سیستم شما نسبت به این اکسپلویت آسیب‌پذیر نمی‌باشد .
   - این اسکریپت فقط نصب این آپدیت را چک می‌کند، همواره سعی کنید سیستم خود را آپدیت نگهدارید.
3. اما اگر پیام قرمز رنگ «System is NOT Patched» را مشاهده کردید لازم است به بخش راهکارها مراجعه و آپدیت را دریافت و نصب نمایید.

جهت اجرای این اسکریپت لازم است Powershell 2.0 یا بالاتر روی سیستم شما نصب باشد. جهت تست در ویندوزهای قدیمی‌تر از سایر روش‌های قید شده در سایت میکروسافت بهره بگیرید.

روش تست کل شبکه (مخصوص مدیران شبکه)

در این روش کل سیستم‌های شبکه برای وجود/عدم وجود آسیب‌پذیری تست می‌شوند. در این مقاله از اسکریپت NMap جهت پویش آسیب‌پذیری استفاده شده است:

یک سیستم را که به پورت 445 سایر سیستم‌ها دسترسی دارد انتخاب نمایید.

نرم‌افزار nmap را دانلود و نصب نمایید. (نسخه ۷.۷۰ به بالا)

دستور زیر را در کامندلاین ویندوز اجرا نمایید:

```
nmap -Pn -sS -p445 --open --max-hostgroup 3 --script smb-vuln-ms17-010.nse --script-args vulns.short -v <ip-address-range> | findstr "VULNERABLE smb-vuln-ms17-010: report"
```

عبارت <ip-address-range> را با رنج آی‌پی مدنظر خود (مثلا 24/192.168.1.0) جایگزین کنید.

دقت کنید که در این روش شما در واقع یک پیش‌حمله شبیه‌سازی شده را انجام می‌دهید که امکان دارد توسط سیستم‌های امنیتی در شبکه شما تشخیص و جلوگیری شود.

در نتیجه قبل از اجرا، لازم است تنظیمات فایروال و شبکه شما اجازه این دسترسی را داده باشند. همچنین اگر سامانه تشخیص نفوذ (IPS) در شبکه دارید یا ضدویروس شما مجهز به این امکان است، برای نتایج دقیقتر و جلوگیری از جاافتادن سیستم‌ها لازم است آنها را طوری تنظیم کنید که اجازه حمله از طریق سیستم انتخاب شده را بدهد.

راهکار اصلی مقابله با آلودگی (نصب آپدیت)

اگر سیستم شما آسیب‌پذیر است لازم است ویندوز خود را آپدیت نمایید.

طبیعتا ما توصیه می-کنیم همواره همه وصله-های امنیتی را نصب کنید و بروز باشید. بهترین راه برای این کار این است که مکانیزم آپدیت خودکار ویندوز فعال باشد و کار کند. اما برای کاربرانی که ویندوزشان به اینترنت متصل نیست، یا به هر دلیلی آپدیت ویندوز را غیرفعال کرده-اند، روش زیر جهت نصب آپدیت توصیه می-شود:

به صفحه MS17-010 در سایت میکروسافت مراجعه کنید.

از جدول موجود در این صفحه، شماره نسخه ویندوز خود را با دقت انتخاب کنید.

مثلا اگر ویندوز ده دارید، بسته به 32 بیت یا 64 بیتی بودن سیستم و اینکه آپدیت 1511 یا 1607 هستید یا خیر باید بسته مناسب را انتخاب کنید. نسخه ویندوزتان را می‌توانید با زدن همزمان کلیدهای Win+R و اجرای برنامه msinfo32 ببینید.

اما اگر در مورد نسخه ویندوز خود شک دارید، می‌توانید چند آپدیت را دریافت کرده و امتحان کنید.

بعد از پیدا کردن شماره نسخه ویندوز، روی آن کلیک کنید) .مثلا Windows 7 for 32-bit Systems Service Pack 1)

در صفحه جدید یکباردیگر نام ویندوز خود را پیدا کنید و فایل مربوطه را دانلود کنید.

سپس فایل را روی ویندوز خود نصب کرده و در صورت نیاز حتما سیستم را ریستارت کنید.

راهکارهای موقت و جایگزین

اگر امکان نصب وصله را ندارید، می‌توانید موقتا از روش‌های زیر برای رفع خطر آلودگی استفاده کنید.

روش بستن File Sharing ویندوز

راه درست این است که ویندوز خود را آپدیت کنید. اما برای کسانی که به دلیلی نمی-توانند آپدیت ویندوز را نصب کنند، بستن File Sharing یک گزینه موقت است.

البته طبیعتا با این کار برخی قابلیت-های ویندوز را از دست خواهید داد، اما برای بسیاری از کاربران این قابلیت استفاده-ای ندارد. حتی اگر آپدیت را نصب کرده باشید بازهم اگر از مکانیزم اشتراک فایل ویندوز استفاده نمی-کنید، خوب است آن را خاموش کنید.

اما این مکانیزم چیست؟

این مکانیزم برای جابجا کردن فایل بین دو سیستم در شبکه استفاده می-شود. مثلا اگر می-خواهید از روی یک سیستم دیگر به فایل-های سیستم خود دسترسی پیدا کنید، استفاده از File Sharing یا Shared Folder اولین کاری است که به ذهن می‌آید. همچنین این مکانیزم برای اشتراک گذاشتن پرینتر در شبکه نیز استفاده می-شود تا سایر رایانه-ها بتوانند از پرینتر سیستم شما استفاده کنند.

دقت کنید که اگر این گزینه را غیرفعال کنید باز هم می‌توانید فولدرها و پرینترهای سایر سیستم‌ها را ببینید و از آن استفاده کنید، اما دیگران قادر به رویت فایل‌ها و پرینترهای به اشتراک گذاشته روی سیستم شما نخواهند بود.

اگر هیچ یک از این‌ها را استفاده نمی-کنید، می-توانید File Sharing را به روش زیر غیرفعال کنید:

برای ویندوز :XP به کنترل پنل ویندوز رفته و گزینه Network Connection را انتخاب کنید.

برای ویندوزهای هفت به بعد: منوی استارت را باز کرده و دنبال گزینه View Network Connectionsبگردید و آن را باز کنید.

در پنجره باز شده روی هر کارت شبکه فعال کلیک راست کرده و Properties را انتخاب کنید.

در پنجره بعدی، گزینه File and Printer Sharing را غیرفعال کنید.

حواستان باشد که غیرفعال کردن یک گزینه موقتی است و باید سیستم خود را حتما بروز کنید.

روش غیرفعال کردن پروتکل SMBv1

به جای غیرفعال کردن کامل File Sharing می‌توانید تنها پروتکل نسخه ۱ که مربوط به این آسیب‌پذیری است را ببندید. با این روش تنها ویندوزهای XP, Server 2003 و ماقبل ارتباط File and Printer Sharing خود را از دست می‌دهند. به علاوه در صورت وجود ارتباط SMB با سیستم‌های لینوکسی قدیمی نیز ممکن است ارتباط قطع گردد.

برنامه regedit را باز کنید.
آدرسHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\را پیدا و باز نمایید.

در بخش سمت راست، به دنبال عبارت SMB1 بگردید و اگر وجود ندارد یک مقدار جدید با این نام از نوع DWORD بسازید.

مقدار آن را برابر صفر (0) قرار دهید.

سیستم را ریست کنید. (تا قبل از ریست سیستم تغییرات اعمال نخواهند شد)

این کار از طریق Group Policy در مسیر Computer Configuration\Preferences folder\Windows Settings\Registry نیز قابل انجام است و کافیست به روش بالا کلید رجیستری را تنظیم نمایید. دقت نمایید که در این روش، باید ابتدا از اعمال Group Policy به کلاینت مطمئن شوید و سپس سیستم ریست شود تا تغییرات اعمال شوند. (بازه معمول اعمال Group Policy هر بیست دقیقه است)

راهکارهای کاهش ریسک در شبکه

جهت کاهش ریسک این آسیب‌پذیری به طور کلی توصیه می‌شود اقدامات زیر در سطح زیرساخت شبکه انجام گیرند:

انجام VLAN بندی کلاینت‌ها، به نحوی که کلاینت‌های هر بخش سازمان با توجه به سطح دسترسی مورد نیاز در یک VLAN مخصوص قرار بگیرند.

همچنینVLAN بندی سرورها، به نحوی که سرورهای دارای کاربرد متفاوت در بخش‌های جدا قرار بگیرند. بخصوص سرورهای متصل به اینترنت و بدون اینترنت جدا شده و نیز سرورهای قابل دسترس از اینترنت در VLAN جدا قرار بگیرند.

تنظیم سیاست‌های شبکه به نحوی که کلاینت‌های بی‌ربط یکدیگر را نبینند.

تنظیم سیاست‌ها به نحوی که ارتباط بینVLAN ها فقط برحسب پورت و پروتکل لازم انجام گرفته و سایر پروتکل‌ها بسته شوند.

نصب ضدویروس دارای امکان IPS و اطمینان از عملکرد آن در شبکه

پیگیری گزارشگیری از سیستم ضدویروس جهت یافتن کلاینت‌های آلوده و برطرف کردن آلودگی (در کنسول پادویش از طریق گزارش Custom Report\IDS – Top Sources Of Attack می‌توانید لیست آی‌پی‌های حمله‌کننده را بیابید)

این آسیب‌پذیری با نام‌های WannaCry و CVE.2017.0146 در سیستم IPS پادویش شناسایی و جلوگیری می‌شود.

پایان.