باج‌گیر افزار چیست و چرا WannaCry این‌قدر خطرناک است؟

باج‌گیر افزار نوعی ویروس کامپیوتری است که معمولاً از طریق اسپم‌های قرار داده شده در پست‌های الکترونیک و لینک‌های دانلود مخرب گسترده می‌شود و به‌طور خاص برای قفل کردن فایل‌های موجود بر روی کامپیوتر مورد هدف طراحی شده است تا اینکه قربانی میزان باج درخواستی را پرداخت کند که معمولاً مبلغی بین ۳۰۰ تا ۵۰۰ دلار آمریکاست و به‌صورت رمز ارز از قربانی گرفته می‌شود.

اما چه چیزی WannaCry را خاص و بسیار مخرب کرده است؟ دلیل این امر توانایی گسترده شدن این باج‌گیر افزار به‌صورت خود به خودی و بدون نیاز به کلیک کردن بر روی لینک یا فایل به خصوصی است.

باج‌گیر افزار WannaCry که به Wanna Decryptor نیز مشهور است از یک بهره‌بردار SMB در ویندوز به نام EternalBlue استفاده می‌کند که به یک مهاجم از راه دور اجازه می‌دهد تا به یک کامپیوتر دارای سیستم‌عامل ویندوز که وصله نشده است نفوذ کند.

هنگام آلوده شدن سیستم قربانی، WannaCry شروع به جستجو برای پیدا کردن دیگر کامپیوترهای آسیب‌پذیر در شبکه مشابه می‌کند و همین‌طور میزبان‌هایی را به‌صورت تصادفی در اینترنت جستجو می‌کند تا بتواند به‌سرعت گسترش پیدا کند.

باج‌گیر افزار

این حملات از روز جمعه ۱۲ می ۲۰۱۷ آغاز شد و چندین بیمارستان در سراسر جهان مورد حمله این باج‌گیر افزار قرار گرفته‌اند و آن‌ها درنهایت مجبور شدند کل سیستم IT خود را در آخر هفته خاموش کنند و قرارهای بیماران و عمل‌های جراحی از پیش برنامه‌ریزی شده را کنسل کردند.

این حمله سایبری بسیاری از سازمان‌ها را تحت تأثیر قرار داده و از پای درآورده است.

در اینجا جزئیاتی که در قبل منتشر شده است مجدداً آورده نشده و شما می‌توانید مقالاتی که در گذشته منتشر شده است را برای کسب اطلاعات بیشتر مطالعه کنید:

روز اول (آغاز انتشار این باج‌گیر افزار): WannaCry بیش از ۹۰،۰۰۰ کامپیوتر را در ۹۹ کشور مورد حمله قرار داد.

روز دوم (روز انتشار وصله‌ها): یک محقق امنیتی به‌طور موفقیت‌آمیز راه‌حلی را کشف کرد تا سرعت آلوده شدن توسط این باج‌گیر افزار را کاهش دهد و مایکروسافت وصله‌های ضروری را برای نسخه‌هایی از ویندوز که دیگر تحت حمایت قرار ندارند منتشر کرد.

روز سوم (انتشار نسخه جدید): نسخه جدیدی از باج‌گیر افزار WannaCry منتشر شد که همراه و یا بدون kill-switch بود و در سطح اینترنت پخش و شناسایی شد که در طی چند هفته آینده متوقف کردن آن به‌شدت سخت خواهد بود.

این تازه آغاز کار بود. محققان امنیتی نسخه‌های جدیدتری از این باج‌گیر افزار را کشف کرده‌اند که WannaCry 2.0 نام‌گذاری شده است و از طریق kill switch متوقف نمی‌شود.

چیزی که بدتر بود این است که نسخه جدید WannaCry منتشر شده احتمالاً توسط شخص دیگری ساخته شده بود و نه توسط مهاجمینی که در پشت باج‌گیر افزار اصلی WannaCry قرار داشتند.

این‌طور حدس زده می‌شود که دیگر گروه‌های مجرمان سایبری و همین‌طور script-kiddieها توسط این باج‌گیر افزار انگیزه گرفته‌اند تا باج‌گیر افزارهای مخرب مشابه را تولید و پخش کنند.

چه کسی در پشت WannaCry قرار دارد و چرا باید یک فرد این کار را انجام دهد؟

درحالی‌که هنوز مشخص نیست چه کسی در پست WannaCry قرار دارد که احتمال دارد مهاجمان سایبری در مقیاس بزرگ باشند که گاهی اوقات توسط دولت‌ها حمایت می‌شوند، اما این حملاتِ در حال انجام هیچ‌گونه لینکی به دولت‌های خارجی ندارند.

یورو پل یا آژانس پلیس اتحادیه اروپا در این مورد گفته است: "حمله اخیر در سطح بی‌سابقه‌ای انجام شده است و نیازمند تحقیقات بین‌المللی پیچیده برای شناسایی مجرمان است."

چرا افراد پشت این باج‌گیر افزار صدها و هزاران کامپیوتر را در سراسر جهان مورد حمله قرار دادند؟ جواب این سؤال ساده است، تا از کاربران آلوده شده پول بیشتری اخاذی کنند.

بیت کوین

با بررسی نرخ گسترده شدن این باج‌گیر افزار، به نظر می‌رسد مجرمانی که در پشت این حمله قرار داشتند هزاران دلار تابه‌حال دریافت کرده‌اند اما بر طبق گزارش‌ها یک کاربر به نام @actual_ransom در توییتر که جزئیات هر نقل و انتقالی را منتشر می‌کند، این مهاجمان به‌طور عجیبی در راه کسب منافع خود از این باج‌گیر افزار ضعیف عمل کرده‌اند.

تا تاریخ ۱۵ می ۲۰۱۷، مهاجمان WannaCry 171 پرداختی دریافت کرده‌اند که مجموعاً برابر با ۲۷٫۹۶۹۶۸۷۶۳ بیت کوین بوده است.

وصله مربوط به آسیب‌پذیری SMB را نصب کنید.

ازآنجاکه باج‌گیر افزار WannaCry از یک آسیب‌پذیری SMB اجرای کد از راه دوربه نام CVE-2017-0148 بهره‌برداری می‌کند که مایکروسافت در ماه مارس و با انتشار وصله MS17-010 آن را وصله کرد.

علاوه بر این، مایکروسافت در این زمان سخت نسبت به کاربرانش بسیار سخاوتمندانه عمل کرده و این شرکت وصله‌های SMB مربوط به نسخه‌هایی از ویندوز که دیگر حمایت نمی‌شوند شامل ویندوز ایکس پی، ویستا، ۸، سرور ۲۰۰۳ و ۲۰۰۸ را نیز منتشر کرده است[۹].

نکته: اگر شما از نسخه ۱۷۰۳ ویندوز ۱۰ (Creators Update) استفاده می‌کنید نسبت به آسیب‌پذیری SMB آسیب‌پذیر نیستید.

چه کسی مسئول حمله WannaCry است؟

آیا مایکروسافت مسئول این همه خرابی است چرا که سیستم‌عاملی با آسیب‌پذیری‌های زیاد تولید کرده است؟

یا اینکه NSA مسئول است چراکه این آژانس اطلاعاتی ایالات‌متحده آمریکا، این آسیب‌پذیری حیاتی را پیداکرده بود و به‌صورت غیرمستقیم و با عدم گزارش این آسیب‌پذیری به مایکروسافت، موجب تسهیل حملات WannaCry با استفاده از این آسیب‌پذیری شده بود.

یا اینکه مسئولیت این فاجعه بر عهده مهاجمان گروه Shadow Brokers است که به سرورهای NSA حمله کرده اما به‌جای گزارش پیدا کردن این آسیب‌پذیری به مایکروسافت، آن‌ها تصمیم به انتشار این ابزارهای حمله و بهره‌بردارهای روز صفر در سطح اینترنت و عموم گرفتند.

یا شاید کاربران ویندوز در این مسئله مقصر باشند که وصله‌های امنیتی موردنیاز را بر روسی سیستم‌های خود نصب نکرده‌اند و یا اینکه هنوز از نسخه‌هایی استفاده می‌کنند که دیگر توسط مایکروسافت پشتیبانی نمی‌شود.

معلوم نیست که چه کسی را جهت این حملات باید سرزنش کنیم، اما تمام موارد بالا می‌توانند در گسترده شدن این حملات به‌طور مساوی سهیم باشند.

مایکروسافت NSA و CIA را جهت حملات سایبری WannaCry سرزنش می‌کند.

مایکروسافت دولت ایالات‌متحده آمریکا را به جهت کمک کردن به این حملات سایبری مانند WannaCry توسط افشا نکردن این آسیب‌پذیری‌ها در ویندوز به سازندگان آن‌ها و نگه‌داشتن آن‌ها جهت بهره‌برداری شخصی از آن‌ها مانند حملات جاسوسی سایبری در سطح جهان مقصر می‌داند.

در یک گزارش که در روز یک‌شنبه ۱۴ می ۲۰۱۷ منتشر شده است، مدیرعامل مایکروسافت یعنی Brad Smith سازمان‌های اطلاعاتی آمریکا را به اعمال غیراخلاقی محکوم کرد و گفت که گسترده شدن این خسارت که توسط WannaCry صورت گرفته است به علت نگه‌داشتن آسیب‌پذیری‌های روز صفر توسط NSA، CIA و دیگر سازمان‌های اطلاعاتی و اجازه دادن به دزدیده شدن آن‌ها توسط مهاجمان است.

Smith می‌گوید: "این یک الگوی در حال ظهور در سال ۲۰۱۷ است. ما دیدیم که آسیب‌پذیری‌هایی که توسط CIA مخفی نگه داشته شده بود توسط WikiLeaks منتشر شد و در حال حاضر نیز آسیب‌پذیری‌هایی از NSA دزدیده شده است که بر روی کاربرانی در سراسر جهان تأثیر گذاشته است."

این بیانیه به‌صورت عمومی تأیید کرد که ابزارهای حمله و بهره‌بردارهای منتشر شده توسط Shadow Brokers به Equation Group تعلق داشته است که در حقیقت یک گروه از مهاجمان نخبه هستند که برای NSA کار می‌کنند.

Smith همچنین اضافه کرده است: "به‌صورت مکرر، بهره‌بردارهایی که در دست دولت است در اختیار عموم قرار می‌گیرد و باعث خرابی‌های فراوان می‌شود."

هنگامی‌که باج‌گیر افزار WannaCry در روز جمعه ۱۲ می کار خود را آغاز کرد و ۳۰،۰۰۰ کامپیوتر را در سراسر جهان آلوده کرد، در آن زمان هیچ‌کس نظری در مورد اینکه چه اتفاقی در حال افتادن است، نداشت و هیچ‌کس نمی‌دانست این باج‌گیر افزار چگونه با این سرعت در حال گسترده شدن است.

از آن موقع تابه‌حال، بعضی از متخصصان امنیت سایبری و شرکت‌ها به‌صورت شبانه‌روزی سخت در تلاش بودند تا نمونه‌های این بدافزار را آنالیز کنند تا بتوانند جلوی این حمله بزرگ را بگیرند.

در اینجا چند نفر نام برده می‌شوند که میلیون‌ها کامپیوتر را از خطر حمله این باج‌گیر افزار نجات دادند:

MalwareTech: شکارچی بدافزار ۲۲ ساله و بسیار حرفه‌ای که برای اولین بار kill swith را کشف کرد که اگر مورداستفاده قرار می‌گرفت جلوی گسترش این بدافزار را می‌گرفت.

Matthieu Suiche که یک محقق امنیتی است و در ابتدا دامنه دوم kill switch را در نسخه‌های دیگر WannaCry کشف کرد و تقریباً ۱۰،۰۰۰ کامپیوتر را نجات داد.

Costin Raiu که یک محقق امنیتی در کاسپرسکی است و اولین نفری بود که کشف کرد انواع مختلف این باج‌گیر افزار در سطح اینترنت وجود دارد که توسط گروهای مهاجم دیگری ساخته شده و توانایی kill-switch را ندارند.