وای! ژوئن 2017

SANS SECURING THE HUMAN
SafeNet Network & Security Services
شبکه امن اندیشه فردا

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- مقدمه
- وصله زدن (Patching)
- پشتیبان گیری(Backup)
- فیشینگ(Phishing) یک روش کلاهبرداری اینترنتی

درسهایی از باج افزار WannaCry

مقدمه

سردبیر مهمان

دکتر ژوهانس اولریچ رییس بخش تحقیقات موسسه SANS و موسس DShield.org میباشد. وی مسئول مرکز **SANS Internet Storm** است که تهدیدات درحال رخ دادن را نظارت میکند. وی همچنین مدرس دوره های Web Application Security (**DEV522**)، (**SEC503**)Intrusion Detection و (**SEC546**) IPv6 میباشد.

به احتمال زیاد اخیرا پوشش وسیعی از خبر حمله سایبری WannaCry را شنیده باشید .این باج افزار بیش از 200 هزار کامپیوتر را آلوده کرده و باعث قفل شدن اطلاعات بسیاری از سازمانها از جمله بیمارستانهایی در انگستان شد. دلایل متعددی وجود دارد که چرا این حمله توجه بسیاری را جلب کرد. دلیل اول، گسترش سریع آن از یک کامپیوتر به کامپیوتر دیگر بدلیل یک ضعف شناخته شده در کامپیوتر های ویندوز بود. دلیل دوم به علت نوع این بدافزار بود که باج گیرنده نامیده میشود یعنی در صورت آلوده شدن کامپیوتر شما کلیه فایلهای شما را رمزگذاری کرده و همه داده های شما قفل میشود. در این صورت تنها راه بازیابی داده ها استفاده از پشتیبان قبلی و یا پرداخت 300 دلار به باج گیر و رمزگشایی داده ها است. علت سوم این است که این حمله میتوانست هرگز اتفاق نیافتد. ضعفی که باج گیر WannaCry از آن برای حمله استفاده کرد ماه ها قبل توسط مایکروسافت شناسایی شده بود و وصله(patch) مربوط به آن نیز ارائه شده بود اما بسیاری از سازمانها در نصب آن کوتاهی کردند، و یا همچنان از سیستم عاملی چون Windows XP استفاده میکنند که بسیار قدیمی است و وصله (patch) جدیدی برای آن ارائه نمیشود. در ادامه سه قدم بسیار آسان به شما پیشنهاد میشود که با استفاده از آنها حملاتی نظیر WannaCry هرگز شما را دچار دردسر نخواهند کرد.

وصله کردن (Patching)

اولین و مهمترین قدم این است که همیشه از به روز بودن کامپیوتر ها، موبایل ها، برنامه ها و هر چیزی که به اینترنت متصل است اطمینان حاصل کنید. مجرمان سایبری دائما در حال جستجو و یافتن ضعف های امنیتی برنامه هایی هستند که توسط سخت افزارهای شما استفاده میشود. در صورت یافتن نقاط ضعف، از برنامه های مخصوص جهت هک کردن و نفوذ به سخت افزار های شما استفاده میکنند. در عین حال شرکتهایی که شما از برنامه های آنها بر روی دستگاه خود استفاده میکنید نیز به شدت در حال کار کردن هستند تا این نقاط ضعف را با ارائه بروز رسانی های جدید از بین ببرند. با بروز رسانی کامپیوترها و موبایل های خود مطمئن باشید کار را برای مجرمان سایبری و هکرها بسیار سخت خواهید کرد. دلیل اصلی گسترش باج افزار WannaCry عدم بروز رسانی بوده است. مایکروسافت تقریبا دو ماه قبل با انتشار آپدیت مربوط به این حمله، امکان جلوگیری از بروز آن را فراهم کرده بود. درصورتیکه سازمانها کامپیوترهای خود را بروز نگه میداشتند، این حمله تحت هیچ شرایطی قادر به کار کردن نبود. برای اطمینان از اینکه دستگاه های شما دارای آخرین آپدیت هستند، بخش بروز رسانی خودکار(automatic

درسهایی از باج افزار WannaCry

update) را در صورت امکان فعال کنید. این امکان نه تنها بر روی کامپیوتر و موبایل شما قابل پیاده سازی است بلکه بر روی اکثر تجهیزاتی که امکان اتصال به اینترنت را دارند نظیر تلویزیون های قابل اتصال به اینترنت، روترهای خانگی، کنسول های بازی، حتی شاید اتوموبیل شما هم وجود دارد. اگر سیستم عامل و یا دستگاهی که از آن استفاده میکنید مانند Windows XP به دلیل قدیمی بودن از قابلیت بروز رسانی برخوردار نیستند، آن را با مدل های جدید که این قابلیت را دارند عوض کنید.

کلید محافظت از خود در برابر حملاتی نظیر WannaCry سه قدم بسیار ساده است: کامپیوتر خود را بروز نگه دارید، مراقب حملات از نوع فیشینگ باشید و از سیستم های خود پشتیبان بگیرید.

پشتیبان گیری

حملا سایبری نظیر باج افزار ها در پاره ای موارد ممکن است سیستم های به روز را نیز آلوده کنند. راه دوم جهت محافظت از اطلاعات، گرفتن پشتیبان از داده هاست. منظور از پشتیبان، کپی کردن اطلاعات در جایی به غیر از کامپیوتر و یا موبایل است. در صورت از دست دادن اطلاعات ارزشمند خود میتوانید با استفاده از فایلهای پشتیبان، آنها را بازیابی کنید. متاسفانه علیرغم سادگی و کم هزینه بودن پشتیبان گیری، افراد بسیاری در انجام آن کوتاهی میکنند. دو راه برای گرفتن پشتیبان وجود دارد: رسانه فیزیکی یا ذخیره سازی ابری. هرکدام از این رویکردها دارای معایب و مزایای خاص خود است. اگر مطمئن نیستید که از کدام روش استفاده کنید میتوانید هر دو رویکرد را بطور همزمان بکار بگیرید. رسانه فیزیکی تجهیزاتی هستند که شما کنترل آن را در دست دارید نظیر حافظه های USB خارجی(External USB drive) یا حافظه های تحت شبکه که در خانه و یا محل کار شما وجود دارد. استفاده از رسانه فیزیکی شخصی این مزیت را دارد که شما قادر خواهید بود که حجم زیادی از اطلاعات را با سرعت بالا بازیابی کنید و یا از آن پشتیبان بگیرید. از معایب این روش این است که اگر سخت افزار شما آلوده به بدافزارهایی مثل باج گیر شود، ممکن است بر روی پشتیبان شما نیز اثر بگذارد و آن را نیز آلوده کند. درصورتیکه از رسانه فیزیکی خودتان برای پشتیبان گیری استفاده میکنید لازم است آن را خارج از سایت و در یک محل امن ذخیره کنید. بر روی هر پشتیبانی که ذخیره میکنید برچسب درست را بچسبانید. راهکارهای ابری(Cloud-based solutions) به سرویس های آنلاینی اطلاق میشود که فایلهای شما بر روی اینترنت پشتیبان گیری و ذخیره میشوند. معمولا برای انجام این کار میبایست برنامه ای بر روی کامپیوتر نصب شود. مهمترین مزیت راهکارهای ابری سادگی آن است. علاوه براین، در صورت آلوده شدن به باج افزار معمولا آلودگی بر روی پشتیبان ذخیره شده در ابر اثری نخواهد داشت. از معایب این راهکار این است که پشتیبان گیری و یا بازیابی داده های با حجم بالا بسیار زمان بر خواهد بود. در خصوص حریم خصوصی و امنیت پشتیبان های ابری بررسی کرده و از درستی عملکرد آن مطمئن شوید. آیا سرویس پشتیبان از امنیت های قوی نظیر رمزگذاری بر روی داده ها و احراز هویت قوی پشتیبانی میکند.

درسهایی از باج افزار WannaCry

فیشینگ

هکرها همیشه در حال بروز رسانی و تغییر روشهای حمله هستند. اغلب مجرمان سایبری از روشی به نام فیشینگ برای حمله و آلوده کردن قربانی استفاده میکنند. فیشینگ زمانی اتفاق میافتد که مجرمان سایبری برای شما ایمیلی ارسال میکنند و با استفاده از حقه هایی شما را ترغیب میکنند که فایل آلوده ای را که پیوست شده باز یا اجرا کنید و یا یک وب سایت مخرب را باز کنید. در صورت انجام این کار ممکن است کامپیوتر شما آلوده شود. اگرچه باج افزار WannaCry از این روش برای حمله استفاده نمیکند ولی بسیاری از حملات دیگر و اکثر باج گیر ها این روش را برای حمله به کار میگیرند. علاوه بر این، مجرمان سایبری که WannaCry را ایجاد کردند، مطمئنا روش های حمله خود را به روز میکنند و در ماه های آتی با تکنیک های جدید نظیر فیشینگ باعث آلودگی کامپیوترهای بیشتری خواهند شد. کلید محافظت از خود در قبال حملات ایمیلی رجوع به عقل سلیم(common sense) است. اگر ایمیلی به نظر عجیب، بسیار مشکوک و یا به نظر فرصتی استثنایی و فریبنده به شما پیشنهاد میکند، به احتمال زیاد یک حمله سایبری است.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه !OUCH شوید و به آرشیو خبرنامه آگاهی از امنیت !OUCH دسترسی داشته باشید، و در مورد راه حلهای افزایش آگاهیهای امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

بدافزار چیست: https://securingthehuman.sans.org/ouch/2016#march2016

باج افزار: https://securingthehuman.sans.org/ouch/2016#august2016

پشتیبان گیری: https://securingthehuman.sans.org/ouch/2015#august2015

فیشینگ: https://securingthehuman.sans.org/ouch/2015#december2015

استفاده امن از ابر: https://securingthehuman.sans.org/ouch/2016#november2016

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی