بولتن تحلیلی ■ بهمن ماه ۱۳۹۸

امنیت اطلاعات

پادویش®
Padvish®
بولتن تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

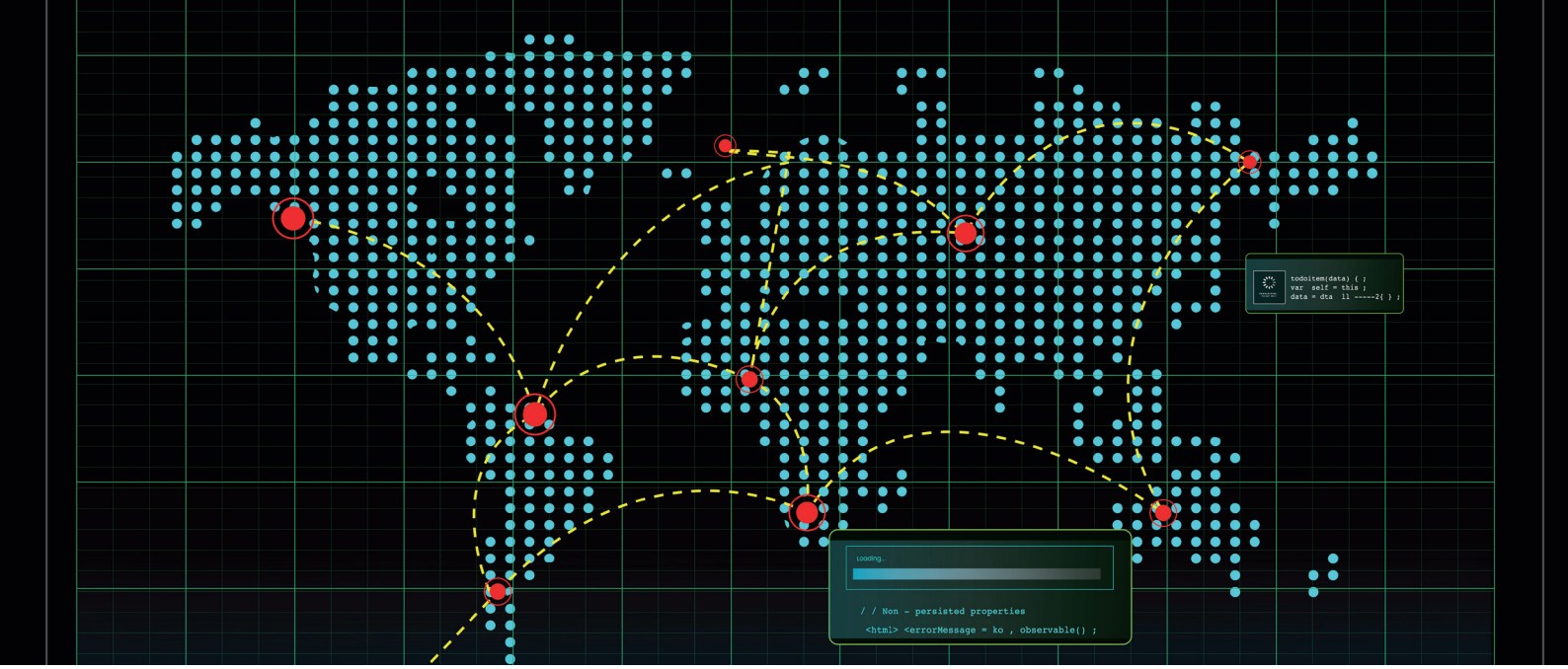
فهرست مطالب

پیش‌گفتار

در خبرنامه بهمن ماه ۹۸ پادویش، به تازه‌ترین اخبار منتشر شده در حوزه امنیت و رویدادهای بدافزاری خواهیم پرداخت.

در ابتدا به یکی از خانواده‌های شایع بدافزاری به نام کرم‌ها و نحوه انتشار آنها می‌پردازیم و یکی از بدافزارهای قدیمی خانواده‌ی کرم‌ها به نام Morto که در سیستم کاربران ایرانی مشاهده شده است را معرفی خواهیم کرد. در ادامه اخبار امن پرداز در ماه گذشته را مرور و بررسی می‌کنیم که شامل انتشار نسخه آزمایشی آنتی ویروس اندروید پادویش می‌باشد. در انتها نیز اصلاحیه‌های منتشر شده در بهمن ماه ۹۸ را به صورت خلاصه گردآوری نموده‌ایم.

هدف از انتشار این ماهنامه، ارائه خلاصه‌ای مفید از اخبار منتشر شده از سوی پادویش در بهمن ماه ۹۸ می‌باشد. امید است در آینده‌ای نه چندان دور، اخباری مدون و جامع از رویدادهای امنیت اطلاعات را به خوانندگان و کاربران محترم عرضه نماییم و در نیل به این هدف از نظرات سازنده و راهگشای شما عزیزان به گرمی استقبال می‌کنیم.



کرم‌ها؛ بدافزارهایی خود تکثیر شونده

کندی غیر معمول سیستم و یا مصرف بی اندازه منابع کامپیوتری از رایج‌ترین مشکلات بین کاربران است. یکی از اولین گمانه‌های موجود، آلودگی بدافزاری سیستم و بویژه آلودگی به کرم‌هاست. اما آیا کرم‌ها به خودی خود وارد سیستم می‌شوند و یا عملکرد ما به عنوان کاربر، ورود آنها را تسهیل می‌کند. برای پاسخ به این سؤال بهتر است درباره ماهیت کرم‌ها بیشتر بدانیم.

کرم های کامپیوتری نوعی بدافزارند که از کامپیوتری به کامپیوتری دیگر پخش می‌شوند. کرم‌ها برای تکثیر نیازی به دخالت انسان‌ها ندارند و بدون اتصال به نرم افزاری خاص و به راحتی وارد سیستم شده و به تخریب منابع می‌پردازند.

کرم‌ها چگونه کار می‌کنند؟

کرم‌ها به روش‌های گوناگونی منتقل می‌شوند. یکی از متداول ترین راه های انتقال آنها، ورود از راه آسیب پذیری‌های نرم افزاری است. روش دیگری که بسیاری از کاربران را آلوده می‌کند، انتقال از راه پیوست ایمیل‌های آلوده یا فایل‌های دریافتی از پیام رسان‌های مورد استفاده و پر کاربرد است. لینک‌های موجود در این فایل‌ها، با آپلود خودکار کرم‌های کامپیوتری، بدون سر و صدا آلودگی را به سیستم کاربر می‌رسانند. با ورود کرم به سیستم، امکان تغییر و حذف فایل‌ها و یا حتی تزریق برنامه‌های مخرب به رایانه فراهم می‌شود.

گاهی تنها هدف کرم از ورود به سیستم شما کپی کردن چندین باره خود و در نتیجه اشغال حداکثری فضای هارد و یا همپوشانی با شبکه‌ی اشتراکی و اشغال پهنای باند است.

خرابکاری کرم‌ها تنها به منابع کامپیوتر کاربر ختم نمی‌شود و برخی انواع پیشرفته تر، داده ها را سرقت می‌کنند، backdoor یا درب پشتی نصب می‌کنند و یا کنترل کامل تنظیمات سیستم قربانی را به هکرها واگذار می‌کنند.

چطور از وجود کرم در سیستم خود باخبر شویم؟

اگر به آلودگی سیستم خود به کرم‌ها مشکوک هستید، اولین راه اسکن کامپیوتر توسط آنتی ویروس‌هاست. حتی در صورتی که نتیجه‌ی اسکن منفی بود، با انجام مراحل زیر می توانید از سالم بودن سیستم خود اطمینان حاصل کنید.

بررسی حافظه سیستم

همان‌طور که در ابتدا اشاره شد، همزمان با تکثیر کرم‌ها، میزان زیادی از حافظه‌ی کامپیوتر اشغال می‌شود. بنابراین یکی از اولین نشانه‌های آلودگی به کرم، مصرف بی اندازه‌ی حافظه است که کندی سیستم را به دنبال خواهد داشت.

گم شدن فایل‌ها

حتما وجود فایل‌های جدید و یا گم شدن فایل‌های قدیمی را جدی بگیرید. عملکرد کرم‌ها به این صورت است که با ورود به سیستم، شروع به پاک کردن فایل‌های میزبان می‌کنند و آنها را با دیگر فایل‌ها جایگزین می‌کنند.

در ادامه به یکی از کرم‌های کامپیوتری به نام Morto که حدود یک دهه از پیدایش آن می‌گذرد و در سیستم کاربران ایرانی نیز مشاهده شده است، می پردازیم.

سوء استفاده از RDP توسط بدافزار Morto

بدافزار Morto از خانواده‌ی کرم‌ها و از جمله بدافزارهای تحلیل شده توسط آزمایشگاه پادویش در سال‌های گذشته است. کرم‌های کامپیوتری همچون Morto، بدون اجازه و اطلاع کاربر وارد سیستم می‌شوند و با هر بار راه اندازی سیستم و یا اتصال به اینترنت، به گسترش خود می‌پردازند. معمولا کرم‌ها به دنبال بخش‌های نامرئی سیستم عامل و مسیرهایی که از دید کاربر پنهان هستند، می‌باشند. نتیجه آن که، زمانی کاربر از حضور این مزاحمان مطلع می‌شود که سیستم کاملا آلوده و کند شده است.

نشانه‌های آلودگی

از جمله نشانه‌های آلودگی سیستم به بدافزار Morto، ایجاد سرویس، تغییر رجیستری‌ها و همچنین اضافه شدن فایل‌های مخرب دیگر به سیستم قربانی است. یکی از مرسوم‌ترین روش‌های انتشار این گونه‌ی مزاحم در شبکه‌ی داخلی سازمان‌ها، سوء استفاده از RDP یا همان قابلیت پرکاربرد دسترسی از راه دور به دسکتاپ است. آلودگی Morto به این سطح ختم نمی‌شود و با رسیدن بدافزار به دیگر سیستم‌های موجود در شبکه، جاسوسی از سیستم قربانی و فرستادن اطلاعات موجود به آدرس‌های از پیش تعیین شده انجام می‌گیرد. در نهایت زمانی کاربر از وجود آلودگی مطلع می‌شود که از سیستم خود و توسط مهاجمان log out شده باشد.

راهکارها

برای در امان ماندن از آلودگی به این نوع بدافزارها، حتما از سالم بودن درایوهای قابل حمل متصل شده به سیستم خود اطمینان حاصل کنید و همچنین از قابلیت RDP با دقت بیشتری استفاده کنید. بخش جلوگیری از نفوذ (IPS) آنتی ویروس پادویش نیز آلودگی‌های احتمالی را شناسایی و از ورود آنها به سیستم قربانی جلوگیری می‌کند.

اصلاحیه‌های منتشر شده در بهمن ماه 98

مهم‌ترین و بحرانی‌ترین اصلاحیه‌ی عرضه شده در روزهای اخیر مربوط به اصلاحیه‌ی RDP Gateway از سوی شرکت مایکروسافت می‌باشد. سایر اصلاحیه‌های ماه ژانویه به شرح زیر می‌باشند:

اجرای کد از راه دور دسکتاپ/ آسیب‌پذیری‌های حملات منع سرویس(DoS)

CVE-۲۰۲۰-۰۶۰۹ و CVE-۲۰۲۰-۰۶۱۰ هر دو از آسیب‌پذیری‌های بحرانی اجرای کد از راه دور (Remote Code Execution) در سرور RDP Gateway به حساب می‌آیند که در صورت سوءاستفاده موفقیت آمیز، مهاجمان می‌توانند کد دلخواه خود را بر روی سرور RDP آسیب دیده اجرا کنند.

CVE-۲۰۲۰-۰۶۱۱ و CVE-۲۰۲۰-۰۶۱۲ نیز سایر آسیب پذیری‌های مرتبط با این گروه می‌باشند.

آسیب‌پذیری در حافظه Internet Explorer

CVE-۲۰۲۰-۰۶۴۰ یکی دیگر از آسیب‌پذیری‌های مهم اجرای کد از راه دور در Internet Explorer است.

آسیب‌پذیری کلاهبرداری CryptoAPI ویندوز

CVE-۲۰۲۰-۰۶۰۱ اشکالی در کتابخانه CryptoAPI به حساب می‌آید که در شرایط خاص به مهاجمی بدل می‌شود که فرایند احراز هویت را دور می‌زند و به اهداف مخرب خود (اتصالات شبکه، پرونده‌ها، ایمیل و اجرایی) اجازه ظاهر شدن با امضای قانونی را می‌بخشد.

آسیب‌پذیری حمله منع سرویس (DoS) در ASP.NET Core

CVE-۲۰۲۰-۰۶۰۲ آسیب‌پذیری موجود در ASP.NET Core که یک فریم‌ورک متن باز است، می‌باشد. این اشکال با توجه به نحوه‌ی رسیدگی به درخواست‌های دستکاری شده، ممکن است منجر به حمله منع سرویس (DoS) گردد.

اصلاحیه های مایکروسافت در ماه میلادی فوریه

مهم‌ترین آسیب پذیری برطرف شده در این شماره، مربوط به آسیب پذیری بحرانی zero-day در اینترنت اکسپلورر و با شناسه‌ی CVE-۲۰۲۰-۰۶۷۴ می‌باشد. اصلاحیه‌ی ماه فوریه، به ترمیم نقص موجود می‌پردازد و به همین خاطر بیش از سایر موارد، توجه کاربران را به خود جلب کرده است.

علاوه بر آسیب پذیری مذکور، ۹۸ مورد دیگر که ۱۱ مورد از آنها به عنوان آسیب پذیری بحرانی طبقه‌بندی شده‌اند نیز منتشر شده است. آسیب پذیری‌های بحرانی منتشر شده، عمدتا مربوط به اجرای کد از راه دور و اختلال در حافظه هستند که شامل سرویس‌های موتور جستجوی اینترنت اکسپلورر، پروتکل دسترسی از راه دور دسکتاپ، فایل‌های LNK و مؤلفه‌های Media Foundation می‌شوند.

آسیب پذیری‌های شرکت سیسکو

سیسکو همانند گذشته به انتشار اصلاحیه‌های ماهانه‌ی مربوط به محصولات خود نموده است. مهم ترین آسیب پذیری‌های منتشر شده به شرح زیر می باشند:

آسیب‌پذیری موجود در Firepower Management Center

این نقص با شناسه CVE-۲۰۱۹-۱۶۰۲۸ و در رابط کاربری مبتنی بر وب نرم افزار Firepower یافت شده است و به عنوان آسیب‌پذیری بحرانی طبقه‌بندی می‌شود. بکارگیری این نقص توسط مهاجمان، امکان ارسال درخواست‌های HTTP دستکاری شده به دستگاه آسیب‌پذیر را فراهم خواهد کرد.

آسیب‌پذیری موجود در Data Center Network Manager

این آسیب‌پذیری به مکانیسم‌های احراز هویت در سیستم "مدیر شبکه مرکز داده سیسکو" (DCNM) و با شناسه‌های CVE-۲۰۱۹-۱۵۹۷۶، CVE-۲۰۱۹-۱۵۹۷۵ و CVE-۲۰۱۹-۱۵۹۷۷ اشاره می‌کند. این نقص منجر به عبور مهاجمان از سدهای کنترل احراز هویت و اجرای کد دلخواه بر روی دستگاه آسیب‌دیده خواهد شد.

آسیب پذیری های اندروید

شرکت گوگل نیز اصلاحیه‌های ماهانه خود را در قالب یک بولتن امنیتی منتشر کرد. در ادامه به مهم‌ترین موارد موجود در اصلاحیه خواهیم پرداخت.

آسیب‌پذیری‌های Framework

شدیدترین آسیب‌پذیری در این بخش به برنامه‌های مخرب محلی اجازه می‌دهد کاربر را فریب دهند و مجوزهای دسترسی پیشرفته‌تری را دریافت کنند. برای دریافت لینک اصلاحیه‌های موجود و مطالعه‌ی جزئیات بیشتر به اتاق خبر امن پرداز مراجعه نمایید.

آسیب‌پذیری در سیستم

شدیدترین آسیب‌پذیری در این بخش، مربوط به آسیب‌پذیری درسیستم بلوتوث اندروید است که اجازه اجرای کد دلخواه و مورد نظر مهاجمان بر روی سیستم آسیب‌دیده را فراهم می‌کند و با شناسه‌ی CVE-۲۰۲۰-۰۰۲۲ منتشر شده است.

آسیب‌پذیری در اجزای کرنل

شدیدترین آسیب‌پذیری در این بخش، منجر به اجرای کد دلخواه مهاجم محلی از طریق بکارگیری فایل‌های خاص و دستکاری شده می‌گردد. برای دریافت لینک اصلاحیه‌های موجود و جزئیات بیشتر به اتاق خبر امن پرداز مراجعه نمایید.

آسیب‌پذیری در اجزای Qualcomm

برای دریافت لینک اصلاحیه‌های مرتبط با اجزای Qualcomm و جزئیات هر کدام به اتاق خبر امن پرداز مراجعه نمایید.

آسیب‌پذیری در اجزای متن بسته‌ی Qualcomm

برای دریافت لینک اصلاحیه‌های مرتبط با اجزای متن بسته‌ی Qualcomm و جزئیات بیشتر به اتاق خبر امن پرداز مراجعه نمایید.

تازه‌های پادویش

با توجه به اتمام مراحل تست آنتی ویروس اندروید نسخه‌ی رایگان پادویش، شرکت امن پرداز کاربران را برای مشارکت در انتشار نسخه جدید دعوت نموده است.

ویژگی‌های نسخه‌ی جدید اندروید:

ظاهری کاملا متفاوت و کاربرپسند

مشاهده‌ی میزان خطر آفرینی برنامه‌ها

افزودن قابلیت‌های برنامه شامل امکان حذف فایل‌های بلااستفاده (Junk Cleaner)

فراهم نمودن امکانات مناسب تر جهت انتخاب مدل پویش از جمله: سریع، کامل، فایل

این نسخه‌ی آزمایشی با حداقل تست‌ها و جهت ارزیابی توسط کاربران پادویش در نیمه بهمن ماه عرضه شد.

برای اطلاعات بیشتر و مطالعه تحلیل فنی و اخبار روز بدافزارها می‌توانید به وب‌سایت‌های تخصصی امن‌پرداز مراجعه کنید:

همچنین برای دریافت هرگونه مشاوره‌ی تخصصی در زمینه امنیت اطلاعات و توسعه نرم‌افزار، از راه‌های زیر با کارشناسان ما در ارتباط باشید:

۰۲۱-۴۳۹۱۲۰۰۰

support@amnpardaz.com

https://t.me/padvishsecurity

https://sapp.ir/padvishsupport

WWW.PADVISH.COM