خبرنامه تحلیلی پادویش ■ مهر ماه ۱۳۹۹

امنیت اطلاعات

پادویش®
Padvish®

خبرنامه تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

امنیت اطلاعات

فهرست مطالب

مقدمه ۳

چرا نباید به هر اپلیکیشنی در google play اعتماد کنیم؟ ۴

اپلیکیشن پیشنهادی هکرها برای دریافت گواهینامه رانندگی ۵

پنهان شدن بدافزار خطرناک در لیست عرضه بانک ملی ۶

کلاهبرداری در واتس اپ با وعده کفش رایگان آدیداس ۷

هر آنچه درباره باج افزارها باید بدانید ۸

اصلاحیه‌ها و آسیب‌پذیری‌ها ۱۱

ارتباط با ما ۱۲

مقدمه

در خبرنامه تحلیلی مهر ماه ۹۹ پادویش، به آخرین اخبار منتشر شده در اتاق خبر امن‌پرداز در حوزه امنیت فضای مجازی و رویدادهای بدافزاری می‌پردازیم.

اخبار این شماره در ۴ بخش تنظیم شده است. در ابتدا تهدیدهای بدافزاری تحلیل شده از سوی آزمایشگاه تحلیل بدافزار پادویش ارائه شده است. سپس، هشدارهای امنیتی منتشر شده را که در ارتباط با انتشار گسترده بدافزار Emotet و انتشار لینک‌های آلوده در پیام رسان محبوب واتس اپ است را بررسی می‌کنیم. در بخش مطالب آموزشی این ماه، باج‌افزارها را به زبانی ساده معرفی می‌کنیم و همچنین با راهکارهای مقابله با آنها آشنا می‌شویم. در انتها نیز، با خبری درباره آسیب پذیری خطرناک ZeroLogon، خبرنامه مهر ماه را به پایان می‌رسانیم.

شما می‌توانید برای مطالعه خبرهای منتشر شده از بدافزارهای تحلیل شده از سوی آزمایشگاه تحلیل بدافزار پادویش و اطلاع از جدیدترین هشدارهای امنیتی به سایت اتاق خبر امن پرداز مراجعه نمایید.

تهدیدها

چرا نباید به هر اپلیکیشنی در google play اعتماد کنیم؟

تروجان‌ها همواره برای ورود به سیستم کاربران، روش‌هایی را به کار می‌برند تا شبیه به برنامه‌های سالم و کاربردی به نظر برسند. اما با ورود به سیستم قربانی، با توجه به هدف از پیش تعیین شده خود، رفتارهای مخربی را پیش می‌گیرند.

Jocker نام یکی از گونه‌های بدافزاری شایع در هفته‌های اخیر و نوعی تروجان اندرویدی است که در ابتدا خود را به عنوان برنامه‌ای برای ارائه خدمات پیام‌رسانی معرفی می‌کند (تعداد زیادی از برنامه‌های مشاهده شده در google play به این بدافزار آلوده بوده‌اند). اما در حقیقت یکی از گونه‌های بدافزاری است که جهت جاسوسی از اطلاعات کاربر وارد سیستم شده و در راستای سرویس‌دهی به سایت‌های تبلیغاتی فعالیت می‌کند.

هدف اصلی این برنامه این است که کاربران را به طور مخفیانه به عضویت سرویس‌های اشتراکی حق بیمه در آورد. برای رسیدن به این هدف، اولین گام دسترسی برنامه به تمامی پیام‌های دریافتی است تا بتواند کد اشتراکی که توسط وب‌سایت برای کاربر ارسال می‌شود را استخراج کرده و خودش این کد را برای وب‌سایت حق بیمه ارسال کند. نتیجه اینکه سرویس حق بیمه برای کاربر بدون اطلاع او فعال شده و هزینه اشتراک پرداخت می‌شود.

> **هدف اصلی این برنامه این است که کاربران را به طور مخفیانه به عضویت سرویس‌های اشتراکی حق بیمه در آورد.**

برای پیشگیری از آلوده شدن گوشی، از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر خودداری کنید و به هنگام نصب آنها، به مجوزهای درخواستی دقت کنید. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

اپلیکیشن پیشنهادی هکرها برای دریافت گواهینامه رانندگی

حضور جاسوس افزار بر روی گوشی به این معناست که تمامی فعالیت‌ها و اطلاعات کاربر توسط هکرهای سازنده بدافزار رصد می‌شود.

جاسوس‌افزارها به شکلی مخفیانه و یا با فریب کاربر و به عنوان برنامه‌ای کاربردی بر روی گوشی نصب می‌شوند. پس از گذشت مدتی کوتاه و ادامه فعالیت مخفیانه خود، اطلاعات مورد نیاز را جمع آوری و برای سازنده بدافزار ارسال می‌کنند.

طبق گزارش آزمایشگاه تحلیل بدافزار پادویش، جاسوس افزار اندرویدی trafikverket که از خانواده بدافزاری agent است، در هفته‌های اخیر مشاهده شده است. این برنامه که با ادعای کمک و راهنمایی به فارسی زبانان کشور سوئد در زمینه اخذ گواهینامه منتشر شده، مانند تمامی جاسوس افزارها به دنبال سرقت اطلاعات گوشی کاربران است. این بدافزار علاوه بر جاسوسی و سرقت، تغییراتی را در سیستم ایجاد می‌کند که شامل این موارد هستند:

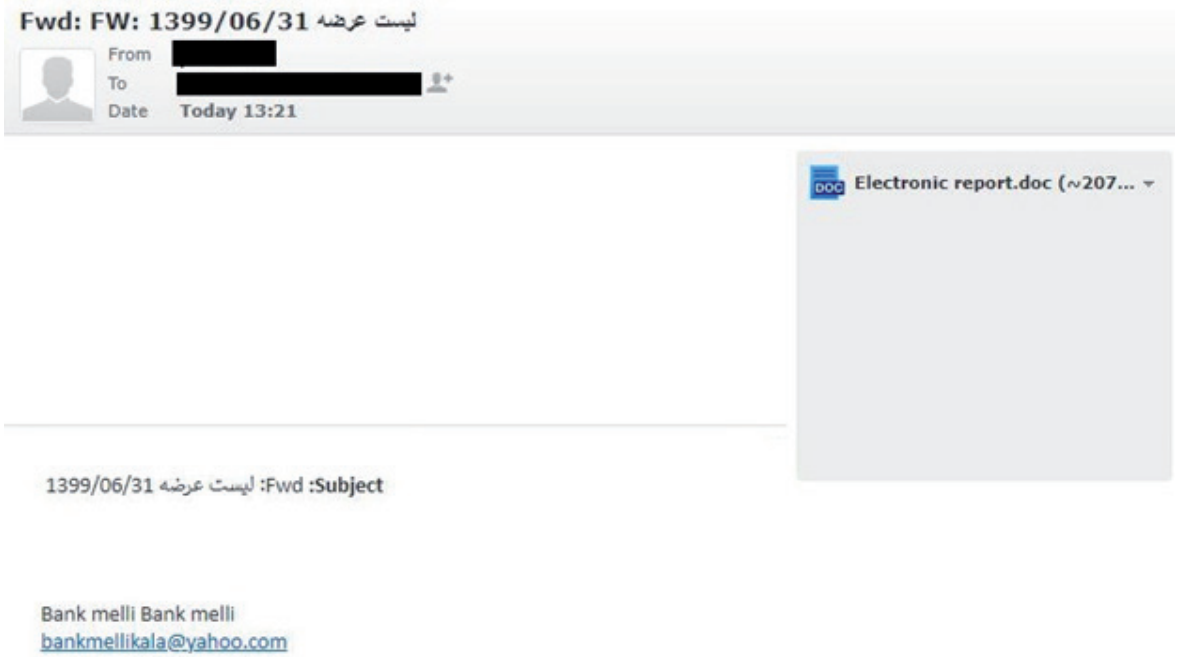
> **پس از گذشت مدتی کوتاه و ادامه فعالیت مخفیانه خود، اطلاعات مورد نیاز را جمع آوری و برای سازنده بدافزار ارسال می‌کنند.**

- ارسال پیام‌های متنی احراز هویت دو مرحله‌ای به شماره تلفنی که توسط سرورفرماندهی و کنترل مهاجم مشخص شده است.
- سرقت اطلاعات از پیام‌های متنی ارسال شده به گوشی کاربر
- سرقت اطلاعات شخصی کاربر مانند جزئیات لیست مخاطبین و حساب‌های کاربری
- ضبط صدای محیط اطراف گوشی کاربر
- فیشینگ حساب کاربری Google
- دریافت اطلاعات دستگاه مانند برنامه‌های نصب شده و یا برنامه‌های در حال اجرا

برای پیشگیری از آلوده شدن گوشی، از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر خودداری کنید و به هنگام نصب آنها، به مجوزهای درخواستی دقت کنید. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

پنهان شدن بدافزار خطرناک در لیست عرضه بانک ملی

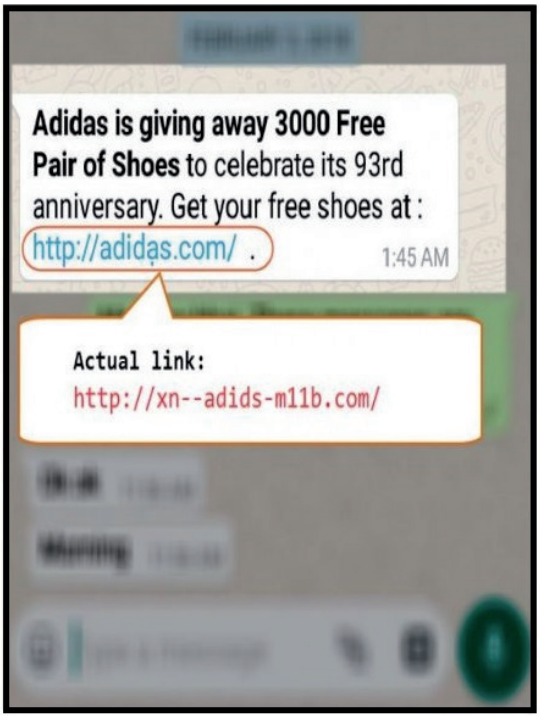
پس از گذشت حدود ۲ ماه از فعالیت مجدد بدافزار Emotet، همچنان ایمیل‌های متعددی که آلوده به نمونه‌های جدیدی از این بدافزار هستند، در سراسر دنیا منتشر می‌شود. به گزارش آزمایشگاه تحلیل بدافزار پادویش، در روزهای اخیر ایمیل‌هایی به زبان فارسی و با عناوینی همچون لیست عرضه بانک ملی و یا تبریک سال نو مشاهده شده است. ویژگی مشترک میان تمامی این پیام‌ها، اتصال فایلی با فرمت ورد (doc) و آلوده به بدافزار Emotet بوده است. بنابراین، در صورتی که ایمیلی با این مضمون و محتوایی مشابه دریافت کردید، از کلیک کردن بر پیوست خودداری کنید. آنتی‌ویروس پادویش ضمیمه بدافزاری این ایمیل را شناسایی و از آلودگی سیستم کاربران جلوگیری می‌کند.



کلاهبرداری در واتس اپ با وعده کفش رایگان آدیداس

به گزارش آزمایشگاه تحلیل بدافزار پادویش، در روزهای گذشته خبری با عنوان آدیداس ۳۱۰۰ کفش ، تی شرت و ماسک رایگان برای همه ارائه می دهد به شکل انبوهی میان کاربران پیام‌رسان واتس‌اپ رد و بدل می‌شود که حاوی لینک مخربی از نوع فیشینگ است.

این خبر که اولین بار در سال ۲۰۱۸ میلادی، با وعده اهدای کفش رایگان و به زبان انگلیسی مشاهده شده بود، به تازگی با تغییراتی جدید و به زبان فارسی منتشر شده است. با باز کردن پیام دریافت شده، به صفحه‌ای با تصویر آدیداس هدایت می‌شوید که در آن شرط دریافت هدایای وعده داده شده، به اشتراک گذاری پیام با حداقل ۲۰ فرد دیگر و یا ۵ گروه در واتس‌اپ، عنوان شده است. متن پیام منتشر شده به شکل روبرو است.



بنابراین، در صورتی که پیامی با محتوای مشابه دریافت کردید، از ارسال مجدد آن و یا باز کردن لینک مشکوک خودداری کنید؛ لینک مخرب بالا توسط افزونه ضد فیشینگ پادویش شناسایی می‌شود.

مطالب آموزشی

هر آنچه درباره باج افزارها باید بدانید

احتمالا بارها با هشدار آلودگی به باج‌افزارها و یا تبلیغات ابزارهای ضد باج‌گیر مواجه شده‌اید و این سوال برایتان پیش آمده که این همه هیاهو و جنجال درباره باج‌افزارها به چه دلیلی است.

طبق آمارهای به دست آمده از وضعیت شیوع باج‌افزارها، پیش بینی می‌شود تا سال میلادی ۲۰۲۱، خسارت ناشی از حملات باج‌افزاری تا ۲۰ میلیارد دلار افزایش پیدا کند. علاوه بر این، بررسی‌ها نشان می‌دهد که تا ماه میلادی سپتامبر سال جاری، بیشترین تهدید سایبری مشاهده شده، از نوع حملات باج‌افزاری بوده است.

بنابراین، لازم است در برابر این تهدید رو به رشد اطلاعات کافی را به دست آورده و آمادگی لازم را داشته باشیم. در ادامه، با این موضوع که باج‌افزارها دقیقا چه کاری انجام می‌دهند، تا چه اندازه خطرناک هستند و البته، راهکارهای مقابله با این نوع آلودگی آشنا می‌شویم.

دقیقا به چه برنامه‌ای باج‌افزار گفته می‌شود؟

باج‌افزارها نوعی بدافزار یا همان برنامه مخرب هستند که از دسترسی کاربر به سیستم یا فایل‌های شخصی جلوگیری می‌کنند و برای بازگرداندن مجوز دسترسی، درخواست باج می‌کنند. باج درخواست شده باید از طریق ارز دیجیتال و یا کارت‌های اعتباری (credit card) پرداخت شود. با این حال، همه باج‌افزارها عملکرد یکسانی ندارند؛ در ادامه با انواع باج‌افزارها آشنا می‌شویم.

انواع باج‌افزارها

باج‌افزارها را به ترتیب شدت و میزان تخریب، به سه دسته کلی زیر تقسیم‌بندی می‌کنند:

۱. Scareware یا ترس‌افزار

این نوع باج‌افزار به اندازه‌ای که اسمش به نظر می‌رسد ترسناک نیست! این برنامه‌ها که به نام نرم‌افزارهای امنیتی فریب‌دهنده نیز شناخته می‌شوند، با نمایش تبلیغات دروغین به کاربر، از کشف بدافزار در سیستم خبر می‌دهند و برای خلاصی از آنها درخواست پول (باج) می‌کنند. در صورت پرداخت نکردن هزینه درخواستی، نمایش تبلیغات ادامه پیدا می‌کند اما فایل‌های سیستم مانند گذشته صحیح و سالم باقی می‌مانند.

۲. Screen lockers یا قفل‌کننده صفحه نمایش

حضور یک باج‌افزار قفل‌کننده صفحه نمایش در کامپیوتر، به معنای قفل شدن صفحه نمایش و عدم دسترسی کاربر به سیستم است. معمولا یک صفحه اخطار بر روی صفحه نمایش قفل شده نشان داده می‌شود که ادعا می‌کند به دلیل در اختیار داشتن محتوای مجرمانه، دسترسی کاربر را به سیستم قطع کرده است و به همین دلیل باید جریمه‌ای را برای ارتکاب کار غیر قانونی پرداخت کند.

۳. باج‌افزارهای رمز کننده

و در نهایت بدترین و خطرناک‌ترین نوع باج‌افزار، باج‌افزارهای رمز کننده

می‌باشند. در این روش، باج‌افزار فایل‌های قربانی را رمز می‌کند و برای ارسال کلید رمز گشایی، درخواست باج می‌کند. علت خطرناک بودن این نوع از باج‌افزارها این است که پس از رمز شدن فایل کاربر، هیچ یک از ابزارهای امنیتی مانند آنتی ویروس‌ها، توانایی بازگردانی فایل قربانی را ندارند. حتی با پرداخت باج، هیچ تضمینی برای بازگرداندن فایل‌ها وجود ندارد.

باج‌افزارها از چه روش‌هایی وارد سیستم می‌شوند؟

اما مهم‌ترین نکته، آگاهی از راه ورود این تهدید به سیستم قربانی است تا از آن جلوگیری کرد. سازندگان بدافزارها پیوسته به دنبال کشف راه‌های تازه‌ای برای ورود به سیستم کاربران هستند که در اینجا، با روش‌های مرسوم ورود باج‌افزارها به سیستم آشنا می‌شویم:

• پورت ریموت دسکتاپ (RDP)

پورت ریموت، امکان ارتباط بین کامپیوترهای مختلف از طریق شبکه را فراهم می‌کند و البته یکی از راه‌های متداول حملات باج‌افزاری است. به طور مثال باج‌افزارهای Dharma و GandCrab و بسیاری دیگر از باج‌افزارها از این راه منتشر می‌شوند. مجرمان سایبری با استفاده از ابزارهای port-scanner کامپیوترهایی که پورت باز دارند را شناسایی می‌کنند و با سوءاستفاده از آسیب‌پذیری‌های موجود در سیستم کاربران و حملات brute force به سیستم مورد نظر نفوذ می‌کنند. مهاجم با غیرفعال کردن آنتی ویروس و بستن دسترسی به فایل‌های پشتیبان، حملات باج‌افزاری خود را آغاز می‌کند.

قابلیت داده‌بان در ضدباج‌گیر پادویش، از اطلاعات شما پشتیبان‌های سبک، کم‌حجم و سریع تهیه می‌کند و از حذف این پشتیبان‌ها در اثر حملات بدافزاری جلوگیری می‌کند.

راه‌های جلوگیری از ورود باج‌افزار

• استفاده از رمز عبور قوی برای پورت ریموت

• پورت ریموت را از حالت پیش فرض (۳۳۸۹) به پورت دیگر تغییر دهید.

• تنها در زمان‌های ضروری از پورت ریموت استفاده کنید و در سایر مواقع آن را بسته نگه دارید.

• احراز هویت دو مرحله‌ای را برای ریموت فعال کنید.

• پیوست ایمیل‌ها

باج‌افزارها عمدتا از راه پیوست ایمیل‌های آلوده منتقل می‌شوند. فایل پیوست شده می‌تواند از نوع فشرده (ZIP)، فایل‌های متنی مثل PDF Excel، Word، و انواع دیگر باشد. در برخی موارد با باز شدن فایل پیوست شده، باج‌افزار سریعا مستقر شده و کاربر را از حضور خود مطلع می‌کند. اما در بسیاری اوقات، حمله کننده ممکن است پس از آلوده کردن سیستم، برای مدت زمانی طولانی که گاهی تا ماه‌ها طول می‌کشد برای رمز کردن فایل‌های قربانی منتظر بماند (مانند حمله باج‌افزاری Emotet یا Trickbot). به طور کلی، هر چه زمان و انرژی که سازنده بدافزار برای طراحی و ارسال ایمیل صرف می‌کند بیشتر باشد، ظاهر ایمیل طبیعی‌تر به نظر می‌رسد و احتمال فریب کاربر و باز کردن ایمیل مخرب بالاتر می‌رود.

راه‌های جلوگیری از ورود باج‌افزار

• تنها پیوست ایمیل‌هایی را که از فرستنده آن مطمئن هستید باز کنید.

• پیوست ایمیل را پیش از باز کردن با آنتی‌ویروس اسکن کنید.

• پیوست‌هایی که نیاز به فعال کردن ماکرو دارند را باز نکنید.

• آدرس‌های اینترنتی (URL) مخرب

در این روش، مهاجمان برای انتشار باج‌افزار، لینک‌های مخربی را در پیام‌های ایمیلی و یا پیام‌هایی که از طریق پیام‌رسان‌ها منتقل می‌شوند، جایگذاری می‌کنند. معمولا برای ترغیب هر چه بیشتر قربانی به کلیک کردن بر روی لینک مخرب، از کلماتی با بار معنایی فوری و مهم استفاده می‌شود.

راه‌های جلوگیری از ورود باج‌افزار

پیش از کلیک کردن بر روی لینک، با نگه داشتن موس بر روی آن (hovering) آدرسی که نمایش داده می‌شود را با دقت بررسی کنید.

• نفوذ از راه شبکه

بر خلاف نسخه‌های قدیمی‌تر باج‌افزارها که تنها با دسترسی محلی، یک سیستم را آلوده می‌کردند، نسخه‌های جدیدتر و پیشرفته‌تر، با توانایی انتشار در شبکه، می‌توانند تمامی سیستم‌های متصل به یک شبکه را آلوده کنند و در بدترین حالت، سازمان مورد حمله را فلج کنند. نمونه‌هایی از باج‌افزارها که قابلیت انتشار در شبکه داشته‌اند WannaCry, Petya و SamSam هستند.

ضد باج گیر پادویش با قابلیت محافظت از MBR سیستم، با باج‌گیرهایی همانند petya مقابله می‌کند.

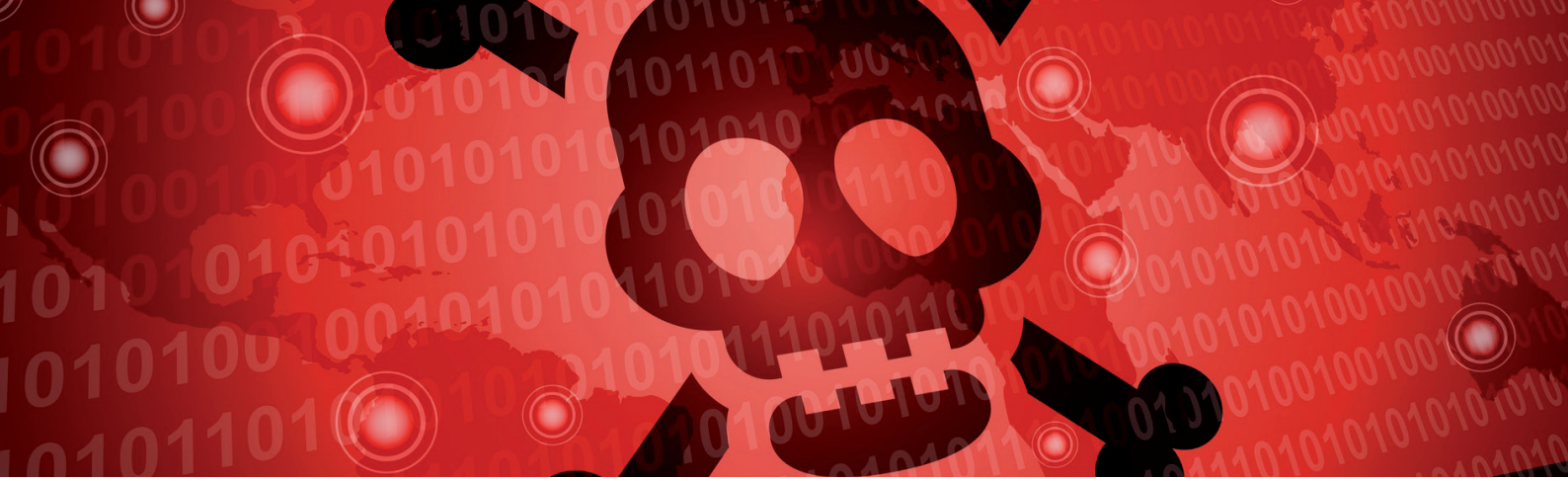
راه‌های جلوگیری از ورود باج‌افزار

• شبکه خود را بخش‌بندی کنید و حداقل دسترسی را برای کاربران به کار ببرید.

• فایل‌های پشتیبان به‌روز و مطمئن برای حمله احتمالی باج‌افزارها تهیه کنید.

• تبلیغات مخرب

تبلیغات مخرب یکی دیگر از روش‌های محبوب سازندگان باج‌افزارها برای



حمله است. خرابکاران از ابزارهای مشابهی که برای تبلیغات سالم و قانونی در اینترنت استفاده می‌شوند، برای تبلیغات محصولات خود بهره می‌برند. تبلیغ نمایش داده شده ممکن است یک تصویر محرک و یا غیراخلاقی، یک اطلاعیه و یا تبلیغ یک برنامه رایگان باشد. با کلیک کردن بر روی تبلیغ، اکسپلویت مخرب، مشخصات مربوط به سیستم کاربر مانند برنامه‌های نصب شده، نوع سیستم عامل، مرورگرهای مورد استفاده و غیره را اسکن می‌کند و در صورت پیدا کردن آسیب پذیری در سیستم، شروع به نصب باجافزار می‌کند. بسیاری از حملات باجافزاری بزرگ مانند CryptoWall و یا Sodinokibi از این روش برای انتشار خود استفاده کرده‌اند.

راه‌های جلوگیری از ورود باجافزار

• سیستم عامل، برنامه‌های نصب شده بر روی سیستم و مرورگرهای خود را به‌روزرسانی کنید.

• پلاگین‌هایی که مورد استفاده نیستند را غیر فعال کنید.

• از برنامه‌های ضد تبلیغ افزار بر روی سیستم خود استفاده کنید.

• دانلود

این روش شامل همه راه‌هایی است که منجر به دانلود مخفیانه و بدون اطلاع کاربر می‌شود. از این روش برای انتشار باجافزار به وسیله آپلود محتوای مخرب در سایت‌های نوشته شده توسط هکرها و یا وب‌سایت‌های قانونی و سالم استفاده می‌شود. با بازدید کاربر از سایت آلوده شده، محتوای مخرب با تحلیل و بررسی آسیب‌پذیری‌های موجود در سیستم قربانی، به صورت خودکار باجافزار را اجرا می‌کند. در این روش، نیازی به کلیک، دانلود و یا نصب هیچ فایلی از سوی کاربر نیست و بازدید از وب‌سایت آلوده، به تنهایی برای آلوده شدن سیستم قربانی کفایت می‌کند.

راه‌های جلوگیری از ورود باجافزار

• همیشه اخرین نسخه از وصله‌های امنیتی نرم افزارها را دریافت و نصب کنید.

• پلاگین‌های غیر ضروری مرورگرها را حذف کنید.

• درایوهای USB

ابزارهای قابل حمل مانند درایوهای USB یکی دیگر از روش‌های جابجایی باجافزارها هستند. اتصال درایو آلوده به یک سیستم، می‌تواند به رمز شدن فایل‌های سیستم محلی منجر شود و همچنین احتمال انتشار باجافزار را در سراسر شبکه به وجود می‌آورد. این اتفاق معمولا به صورت غیر عمدی و ناشی از غفلت کارمندان یک مجموعه در اتصال فلش آلوده به سیستم رخ می‌دهد، اما در برخی موارد و با قصد آلوده کردن یک سازمان، فلش‌های آلوده بین افراد توزیع می‌شود.

راه‌های جلوگیری از ورود باجافزار

• هیچ‌گاه درایوهای قابل حمل ناشناسی که از محتویات آنها اطلاعی ندارید را به کامپیوتر خود متصل نکنید.

• درایوهای قابل حمل شخصی خود را به سیستم‌های عمومی مانند کافی‌نت‌ها و یا دفاتر انتشار متصل نکنید.

• از آنتی‌ویروس مطمئن برای اسکن درایوهای قابل حمل استفاده کنید.

پادویش با دارا بودن قابلیت UMP که جزء محافظت رفتاری آن است، جلوی آلوده شدن سیستم از طریق درایو قابل حمل را می‌گیرد.

در صورتی که سیستم ما به باجافزار آلوده شد چه کار کنیم؟

نکته آخر اینکه، حتی با رعایت همه نکات لازم، ممکن است سیستم ما به باجافزار آلوده شود. در این مواقع بایستی گام‌های زیر را طی کنیم تا با پرداخت کمترین خسارت، فایل‌های مهم خود را بازیابی کنیم:

مهم ترین نکته که در برخورد با باجافزارها باید به خاطر بسپاریم، عدم پرداخت باج به هکرهاست. چرا که با پرداخت باج، به گسترش محصولات سازندگان باجافزارها و به دام افتادن تعداد بیشتری از افراد کمک کرده‌ایم.

به محض اطلاع از آلودگی به باجافزار، سیستم‌های آلوده را شناسایی و اتصال wifi و شبکه‌ای این سیستم‌ها را قطع کنید.

با استفاده از آنتی‌ویروس و یا ابزار ضد باجافزار، سیستم خود را اسکن کنید.

تا پیش از پاکسازی و حذف کامل سیستم از اتصال شبکه و دستگاه‌های ذخیره سازی به سیستم آلوده جدا خودداری کنید.

حتی پاک‌سازی کل سیستم و حذف باجافزار، فایل‌های رمز شده شما را بازگردانی نمی‌کند. بهترین راه حفاظت از اطلاعات باارزش، تهیه فایل‌های پشتیبان به‌روز و مطمئن از داده‌هاست.

اصلاحیه‌ها و آسیب‌پذیری‌ها

کشف خطرناک ترین آسیب پذیری سال 2020؛ تمامی نسخه های ویندوز سرور در معرض خطر هستند

در پی هشدارهای مکرر مراکز فعال در زمینه امنیت سایبری و حوادث باج‌افزاری اخیر در کشور، به گفته بسیاری از کارشناسان، آسیب‌پذیری ZeroLogon خطرناک‌ترین آسیب‌پذیری شناخته شده در سال ۲۰۲۰ است. از این رو، لازم است مدیران شبکه در اسرع وقت سیستم‌های آسیب‌پذیر را شناسایی و نسبت به نصب وصله و رفع آسیب‌پذیری اقدام کنند.

آسیب‌پذیری ZeroLogon که با شناسه آسیب‌پذیری CVE-۲۰۲۰-۱۴۷۲ مشخص شده است، یک آسیب‌پذیری فوق‌العاده خطرناک در تمامی نسخه‌های ویندوز سروری از ۲۰۰۸ تا ۲۰۱۹ است که دارای حداکثر درجه خطر (CVSS ۱۰/۱۰) است.

چرا آسیب‌پذیری ZeroLogon تا این اندازه خطرناک است؟

این آسیب‌پذیری به سادگی قابل وصله کردن نبوده و نصب به‌روزرسانی‌های ویندوز برای محافظت کافی نیست (نصب وصله ممکن است اختلالاتی در عملکرد دامنه ایجاد کند).

کد استفاده از آسیب‌پذیری در اختیار مهاجمان قرار دارد.

استفاده از آسیب‌پذیری بسیار ساده، بدون مشکل و بدون نیاز به اطلاعات هویتی یا ... است.

تمامی نسخه‌های ویندوز سرور آسیب‌پذیر هستند.

آسیب‌پذیری، حداکثر دسترسی (ادمین کل دامنه) را برای مهاجم فراهم می‌کند.

به گفته مایکروسافت، وصله نهایی برای این آسیب‌پذیری در ۳ ماهه ابتدایی سال ۲۰۲۱ ارائه خواهد شد که برای برطرف شدن کامل خطرات این آسیب‌پذیری، نصب آن وصله نیز ضروری است.

نحوه رفع آسیب‌پذیری و نصب وصله

همان گونه که اشاره شد، برای رفع آسیب‌پذیری Zerologon، به‌روزرسانی ویندوز و نصب وصله‌های منتشر شده توسط مایکروسافت به تنهایی کافی نیست. بنابراین، لازم است مدیران شبکه تمامی مراحل زیر را برای رفع مشکل طی کنند:

۱. سیستم‌های DC را آپدیت کنید.

۲. لاگ‌های ویندوز را بررسی کرده و سیستم‌های ناسازگار را بیابید.

۳. سیستم‌های ناسازگار رابه‌روزرسانی یا استثنا کنید.

۴. حالت ارتباط امن را فعال کنید.

پادویش چگونه از کاربران در برابر این آسیب‌پذیری محافظت می‌کند؟

نصب وصله تنها راه مطمئن و قطعی جلوگیری از آسیب‌پذیری است که بایستی انجام گیرد. با این وجود، بخش جلوگیری از نفوذ (IPS) آنتی‌ویروس پادویش نیز اغلب آسیب‌پذیری‌های سیستم عامل ویندوز از جمله آسیب‌پذیری Zerologon را شناسایی و سیستم را در برابر چنین حملاتی ایمن می‌کند.

مختصری درباره امن‌پرداز

شرکت نرم‌افزاری امن پرداز از سال ۱۳۸۳ فعالیت خود را آغاز نموده و به عنوان اولین آنتی ویروس کاملا ایرانی، در جهت برقراری امنیت در فضای سایبری همواره همراه و پشتیبان کاربران خود بوده است. در تلاشیم تا به عنوان مرجعی قابل اعتماد و قابل رقابت با آنتی ویروس‌های خارجی، محصولی متناسب با نیازهای کاربران مختلف خانگی و سازمانی عرضه کنیم. علاقه‌مندان به دریافت اطلاعات بیشتر و مطالعه تحلیل فنی و اخبار روز بدافزارها می‌توانند به وب‌سایت‌های تخصصی امن‌پرداز مراجعه کنند. همچنین برای دریافت هرگونه مشاوره‌ی تخصصی در زمینه امنیت اطلاعات و توسعه نرم‌افزار، از راه‌های زیر با کارشناسان ما در ارتباط باشید:

threats.amnpardaz.com

news.amnpardaz.com

۰۲۱-۴۳۹۱۲۰۰۰

support@amnpardaz.com

https://t.me/padvishsecurity

https://sapp.ir/padvishsupport

WWW.PADVISH.COM