خبرنامه تحلیلی پادویش ■ خرداد ماه ۱۳۹۹

امنیت اطلاعات

پادویش®
Padvish®

خبرنامه تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

امنیت اطلاعات

فهرست مطالب

مقدمه

در خبرنامه تحلیلی خرداد ماه ۹۹ پادویش، تازه‌ترین اخبار منتشر شده در حوزه امنیت فضای مجازی و رویدادهای بدافزاری که در دو بخش تدوین شده است را مرور خواهیم‌کرد.

در ابتدا هشدارهای امنیتی منتشر شده از سوی پادویش را بررسی می‌کنیم که در ارتباط با انتشار سهام عدالت و سوء استفاده‌هایی است که با محوریت این موضوع در حال شکل‌گیری هستند. در قسمت دوم نیز به تهدیدهای بدافزاری تحلیل شده از سوی آزمایشگاه پادویش می‌پردازیم. برای مطالعه بیشتر درباره هر یک از تحلیل‌های فنی ارائه شده می‌توانید به سایت خبری امن‌پرداز که آدرس آن در انتهای گزارش آمده‌است، مراجعه کنید.

هدف از انتشار این خبرنامه تحلیلی، ارائه خلاصه‌ای مفید از اخبار منتشر شده از سوی پادویش در خرداد ماه ۹۹ است. برای مطالعه اخبارهای به‌روز منتشر شده از سوی آزمایشگاه بدافزار پادویش و اطلاع از جدیدترین هشدارهای امنیتی به سایت اتاق خبر امن‌پرداز مراجعه نمایید.

هشدار به دارندگان سهام عدالت

به گزارش آزمایشگاه تحلیل بدافزار پادویش و به نقل از پایگاه اطلاع رسانی پلیس فتا، در روزهای اخیر پیامک‌هایی جعلی با موضوع سهام عدالت و برای دریافت اطلاعات کاربران ارسال شده است. با انتشار خبرهایی از شرایط جدید سهام عدالت، امکان فریب افراد توسط سودجویان به روش‌های گوناگون نیز پدید آمده است. در ادامه به روش‌های کلاهبرداری با محوریت سهام عدالت که تاکنون گزارش شده است، اشاره می‌کنیم:

برای آزاد سازی سهام عدالت نیازی به هیچ‌گونه پرداخت اینترنتی نیست. برخی سودجویان با انتشار پیام‌هایی در فضای مجازی و یا از طریق پیامک، اطلاعات حساب افراد را برای آزادسازی سهام عدالت درخواست می‌کنند و با هدایت آنها به سایت‌های تقلبی و فیشینگ، از حساب بانکی افراد کلاهبرداری می‌کنند. بر روی لینک‌های دریافتی مشکوک کلیک نکنید و از افشای اطلاعات حساب خود خودداری کنید. همچنین اخبار مربوطه را تنها از رسانه‌های رسمی و معتبر دریافت نمایید.

در حال حاضر هیچ‌گونه ثبت نام جدید سهام عدالت صورت نمی‌گیرد. بنابراین مراقب سودجویانی که ادعای ثبت نام از افراد جامانده از سهام عدالت را می‌کنند، باشید.

مراقب تماس تلفنی یا مراجعه حضوری به بهانه سهام عدالت باشید. اطلاع رسانی‌های رسمی درباره سهام عدالت هرگز با این روش‌ها صورت نمی‌گیرند. برای بررسی و دریافت هرگونه اطلاعاتی از سهام خود به سامانه الکترونیکی سهام عدالت مراجعه کنید.

مراقب تماس تلفنی یا مراجعه حضوری به بهانه سهام عدالت باشید. اطلاع رسانی‌های رسمی درباره سهام عدالت هرگز با این روش‌ها صورت نمی‌گیرند.

تهدیدها

تروجان Racealer

بدافزار تروجان نام خود را از اسب چوبی تو خالی که یونانیان در جنگ با تروجان‌ها در آن مخفی شده بودند، اقتباس کرده است. همان طور که تروجان‌ها با دیدن ظاهر فریبنده اسب چوبی به راحتی اجازه ورود دشمن را به درون قلعه خود صادر کردند، قربانیان حملات تروجان‌های کامپیوتری نیز با توجه به ظاهر قانونی و موجه برنامه، بدافزار را دانلود و سیستم خود را آلوده می‌کنند. پیشگیری از حمله تروجان‌ها به سیستم، نیازمند آگاهی کاربر و حفاظت همه جانبه از سیستم مورد استفاده است. فرقی ندارد که از چه دستگاهی استفاده می‌کنید، موبایل، تبلت یا کامپیوتر؛ این نوع از بدافزارها که در قالب برنامه‌های سالم نمایان می‌شوند، خطری برای تمامی سیستم‌ها به حساب می‌آیند.

تروجان‌ها از راه‌های مختلفی به سیستم قربانیان وارد می‌شوند و به شکل‌های مختلفی آسیب می‌رسانند. با آلوده شدن سیستم به تروجان، امکان جاسوسی، سرقت داده‌های با ارزش و ایجاد درب پشتی برای دسترسی‌های بیشتر بر روی سیستم برای مجرمان سایبری فراهم می‌شود.

در اینجا یکی از تروجان‌هایی که منجر به تخریب بالا در سیستم قربانیان می‌شود را معرفی می‌کنیم:

تروجان Racealer یا Raccoon Stealler با هدف سرقت اطلاعات ارزشمند قربانی مانند اطلاعات مرورگرها، walletهای ارزهای دیجیتال موجود در سیستم و اطلاعات ایمیل کاربر، وارد سیستم می‌شود. از آنجایی که هدف این بدافزار سرقت اطلاعات است و نه ایجاد تغییر و خرابکاری در سیستم، بدافزار پس از جمع آوری داده‌های مورد نیاز خود، محل وقوع جرم را بدون باقی گذاشتن اثر قابل توجهی ترک می‌کند. علاوه بر این، در زمان فعالیت، بدافزار تمامی لینک‌ها و IPهای مورد استفاده خود را به سرعت و برای هر حمله تغییر می‌دهد.

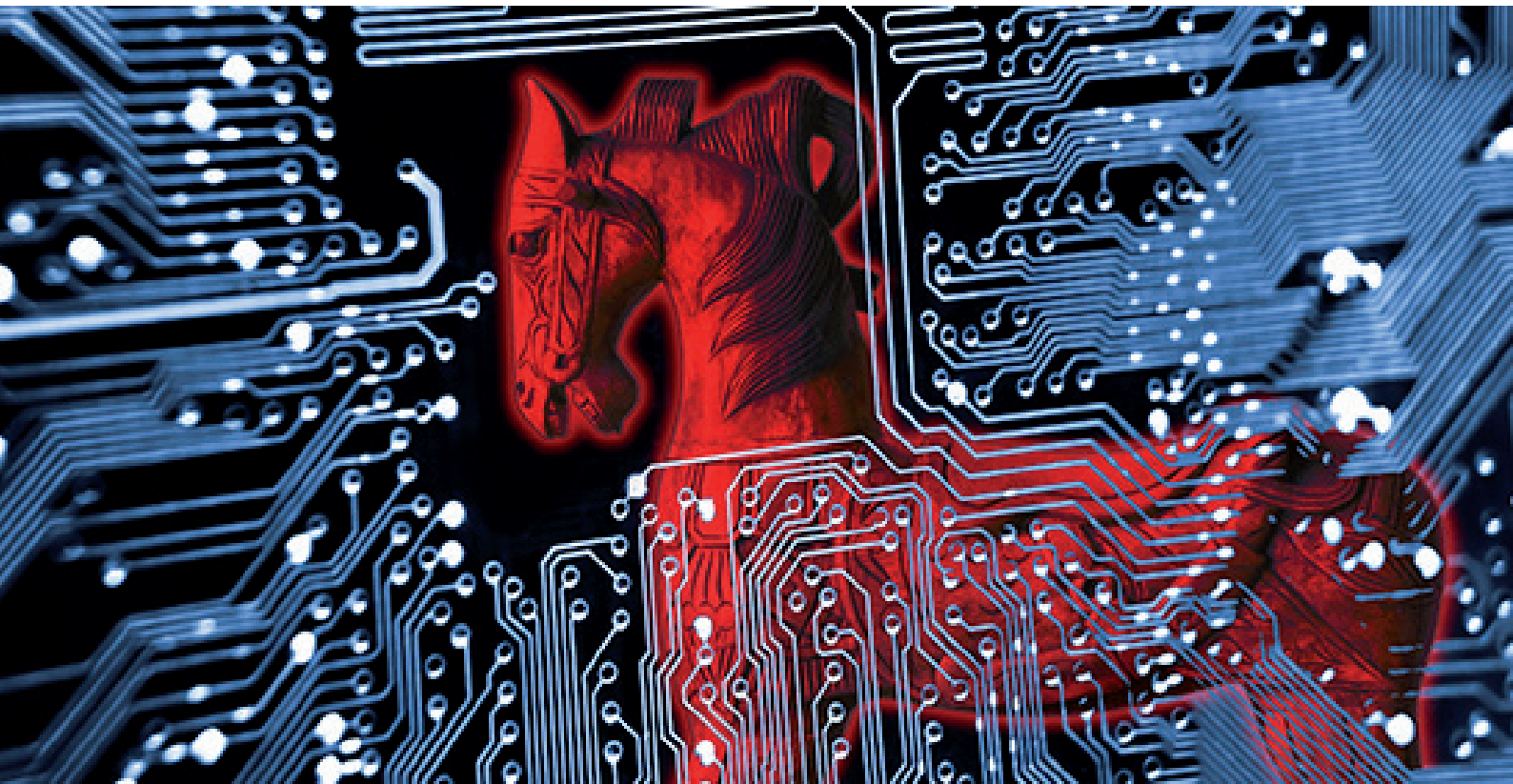
"از آنجایی که هدف این بدافزار سرقت اطلاعات است و نه ایجاد تغییر و خرابکاری در سیستم، بدافزار پس از جمع آوری داده‌های مورد نیاز خود، محل وقوع جرم را بدون باقی گذاشتن اثر قابل توجهی ترک می‌کند."

راه نفوذ بدافزار

روش مرسوم ورود این بدافزار به سیستم، از راه آسیب‌پذیری‌های مرورگر است. بنابراین در صورت امکان همیشه سیستم عامل و مرورگرهای خود را به‌روز نگه دارید و از استفاده از مرورگر Internet Explorer، به خصوص نسخه‌های قدیمی آن که آسیب‌پذیری‌های فراوانی دارد، تا حد امکان خودداری کنید.

روش مقابله و پاک‌سازی سیستم

آنتی‌ویروس پادویش این بدافزار را شناسایی و از سیستم حذف می‌کند. جهت پیشگیری از ورود این نوع از بدافزارها به سیستم پیشنهاد می‌شود از کلیک بر روی لینک‌های مشکوک خودداری نموده و فایل‌های ضمیمه ایمیل‌ها را توسط آنتی‌ویروس پویش نمایید.



جاسوس افزار InfoStealer

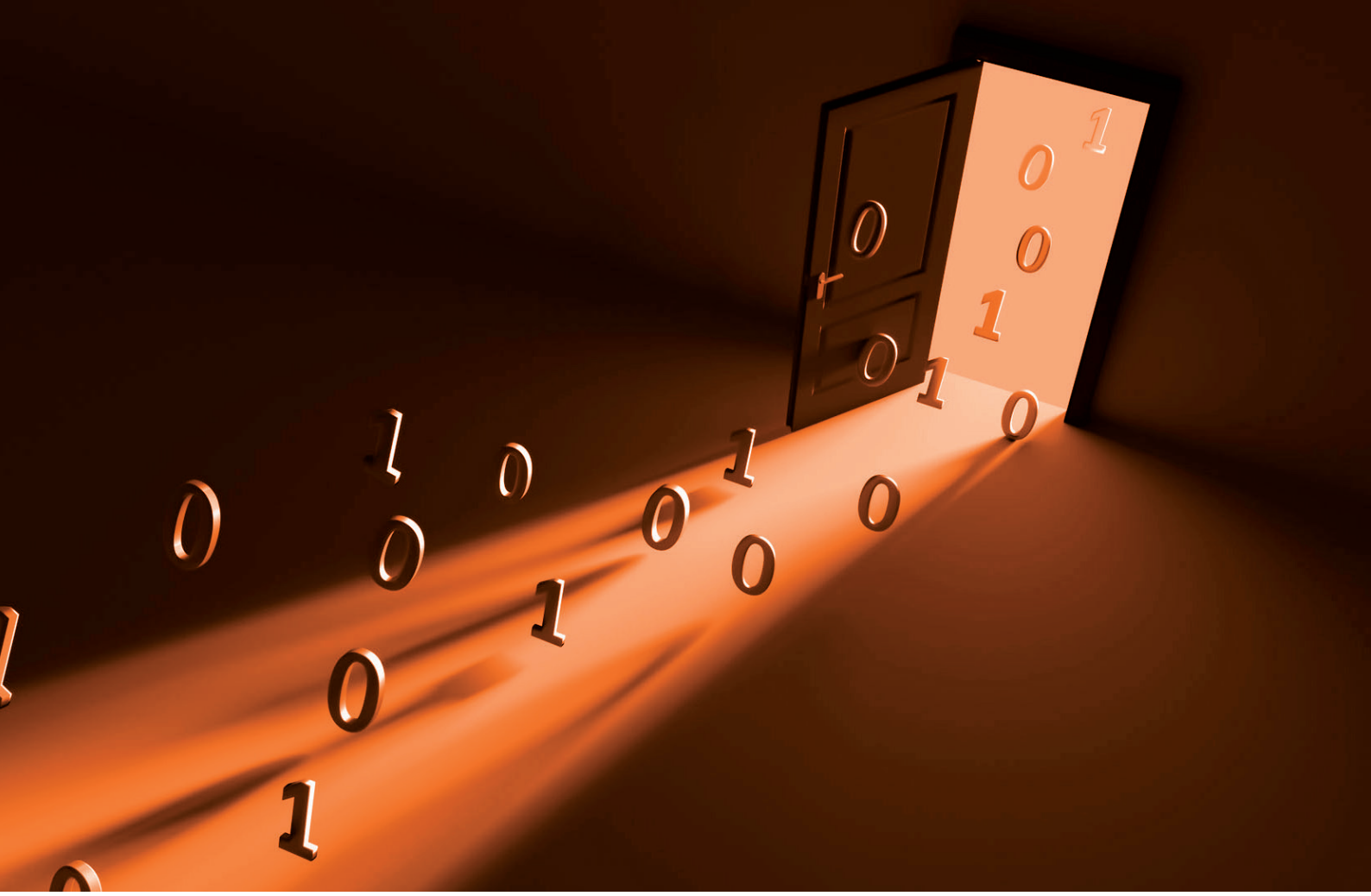
زمانی که با گوشی موبایل خود مشغول گشت و گذار در اینترنت هستید، ممکن است برنامه‌های بسیاری فعالیت شما و اطلاعات شخصی‌تان را زیر نظر داشته باشند. این گونه بدافزارها که برای اهداف جاسوسی و سرقت اطلاعات شخصی و سازمانی کاربران مورد استفاده مجرمان سایبری قرار می‌گیرند، جاسوس افزار نامیده می‌شوند. همان‌طور که انتظار می‌رود، جاسوس افزارها به طور پنهانی وارد سیستم شده و بر روی گوشی نصب می‌شوند و پس از آن نیز به فعالیت مخفیانه خود ادامه می‌دهند. جاسوس افزارها تمامی اطلاعات مورد نیاز در خصوص فعالیت‌های کاربر بر روی گوشی و یا هرگونه اطلاعاتی را جمع‌آوری و در زمان مناسب برای شخص دیگری ارسال می‌کنند.

یکی از خانواده‌های بدافزاری که به تازگی و در زمان همه‌گیری بیماری کووید-۱۹ منتشر شده، جاسوس افزار InfoStealer است. کاربران اندروید با هدف کسب اطلاعات بیشتر درباره بیماری، این اپلیکیشن را نصب می‌کنند و از این راه به هکرها اجازه دسترسی به اطلاعات حساس خود را می‌دهند. با راه‌اندازی این برنامه، تمامی اطلاعات کاربر مانند نوع سیم کارت و مدل گوشی تا متن پیام‌های کوتاه و لیست مخاطبین جمع‌آوری می‌شوند. در شرایطی که بمباران خبری با محوریت ویروس کرونا و اضطراب ناشی از آن تمامی مردم را احاطه کرده است، افراد تمایل بیشتری به نصب چنین برنامه‌هایی دارند و احتمال اینکه این دسته از برنامه‌ها را از منابع یا مارکت‌های غیرمعتبر دانلود کنند بسیار زیاد است. خانواده InfoStealer تنها یک نمونه از مجموعه برنامه‌های جاسوسی با مضمون کووید-۱۹ است.

> **کاربران اندروید با هدف کسب اطلاعات بیشتر درباره بیماری، این اپلیکیشن را نصب می‌کنند و از این راه به هکرها اجازه دسترسی به اطلاعات حساس خود را می‌دهند.**

روش مقابله و پاک‌سازی سیستم

آنتی‌ویروس پادویش این بدافزار را شناسایی و از سیستم حذف می‌کند. جهت پیشگیری از ورود این نوع از بدافزارها به گوشی موبایل، مانند همیشه تاکید بر این است که از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر خودداری کنید و به هنگام نصب برنامه‌های موبایلی، به مجوزهای درخواستی دقت کنید.



درب پشتی PhantomLance

سارقی را تصور کنید که به دنبال فرصتی مناسب برای دزدی از خانه شماست. در حالی که ورودی ساختمان توسط دوربین‌های امنیتی محافظت می‌شود، درب پشتی خانه بدون هیچ قفلی باز است. ادامه ماجرا و دردسرهای پیش رو کاملا قابل پیش‌بینی هستند. بدافزارهای درب پشتی هم با همین شیوه و با بهره‌گیری از نقاط ضعف موجود، به سیستم کاربران نفوذ می‌کنند. هکرها با استفاده از این روش بدون نیاز به اعتبار سنجی وارد سیستم مورد نظر شده و با تغییر نام کاربری و رمز عبور سیستم، کنترل اوضاع را در دست می‌گیرند. با یک بار نفوذ به سیستم، امکان سرقت اطلاعات شخصی قربانی و نصب سایر بدافزارها برای هکر فراهم می‌شود.

به گزارش آزمایشگاه تحلیل بدافزار پادویش، بدافزار اندرویدی Browser Turbo که با نام PhantomLance هم شناخته می‌شود، از سال ۲۰۱۵ مشاهده شده است. این برنامه بدون دخالت کاربر و به سادگی اطلاعات محرمانه‌ای مثل موقعیت مکانی، پیام‌های متنی، لیست تماس‌ها، اطلاعات مربوط به حافظه، لیست برنامه‌های نصب شده و اطلاعات کامل گوشی را از کاربر جمع‌آوری و به سرور خود ارسال می‌کند. با استفاده از قابلیتی که این نوع بدافزار دارد، فیلترهای امنیتی مارکت‌های مختلف اپلیکیشن‌های اندرویدی را دور می‌زند.

> **هکرها با استفاده از این روش بدون نیاز به اعتبار سنجی وارد سیستم مورد نظر شده و با تغییر نام کاربری و رمز عبور سیستم، کنترل اوضاع را در دست می‌گیرند**

روش مقابله و پاک‌سازی سیستم

آنتی‌ویروس پادویش این بدافزار را شناسایی و از سیستم حذف می‌کند. جهت پیشگیری از ورود این نوع از بدافزارها به گوشی موبایل، از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر خودداری کنید و به هنگام نصب برنامه‌های موبایلی، به مجوزهای درخواستی دقت کنید.

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