خبرنامه تحلیلی پادویش ■ تیر ماه ۱۳۹۹

امنیت اطلاعات

پادویش®
Padvish®

خبرنامه تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

فهرست مطالب

مقدمه

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

در ابتدا، هشدارهای امنیتی منتشر شده از سوی پادویش را بررسی می‌کنیم که در این شماره به شیوع مجدد یکی از بدافزارهای قدیمی و راهکارهای مقابله با آن پرداخته شده است؛ جزئیات منتشر شده درباره این بدافزار را در این خبرنامه بخوانید. در ادامه، تهدیدهای بدافزاری تحلیل شده از سوی آزمایشگاه پادویش در تیر ماه را مشاهده می‌کنید. برای مطالعه تحلیل‌های فنی و تخصصی درباره هر یک از بدافزارهای ارائه شده، می‌توانید به بانک اطلاعات تهدیدات بدافزاری پادویش که آدرس آن در انتهای گزارش آمده است، مراجعه کنید.

انتشار خبرنامه تحلیلی پادویش در انتهای هر ماه به منظور ارائه خلاصه‌ای از اخبار منتشر شده توسط پادویش انجام می‌شود. شما می‌توانید برای دریافت اخبار به‌روز از آخرین حملات سایبری و تحلیل‌های منتشر شده از سوی کارشناسان پادویش، به اتاق خبر امن پرداز و صفحه پادویش در شبکه‌های اجتماعی مراجعه نمایید.

هشدار مهم درباره حملات باج افزار GlobeImposter :

پورت های ریموت را ببندید!

به گزارش آزمایشگاه تحلیل بدافزار پادویش، خانواده باج‌افزار GlobeImposter یکی از خانواده‌های مشهور باج‌افزار است که در روزهای اخیر مجددا بسیار فعال شده و در حال آلوده کردن سیستم‌های مختلف در دنیا می‌باشد. این باج‌افزار که در ایران نیز مکررا مشاهده شده است، اخیرا با استفاده از پسوندهای C۱H و C۴H مشغول حملات خود می‌باشد. لازم به ذکر است که در حال حاضر هیچ راهکاری برای بازگردانی اطلاعات رمز شده توسط این باج‌افزار (غیر از استفاده از بکاپ) وجود ندارد.

مطابق بررسی‌های آزمایشگاه تحلیل بدافزار پادویش، علی‌رغم افزایش حملات این باج‌افزار، انواع نسخه‌های جدید مورد استفاده آن در چندین سطح توسط مولفه‌های مختلف تشخیص بدافزار در پادویش شناسایی و به طور کامل جلوگیری می‌شود. اما آنچه این باج‌افزار را خطرناک می‌کند، وجود یک نفوذگر انسانی در پشت آن است که از طریق پورت ریموت دسکتاپ و با استفاده از پسورد ادمین به سیستم‌های شبکه متصل می‌شود. در این موارد، از آنجا که نفوذگر دسترسی کامل به سیستم هدف داشته و حتی پسورد ضدویروس را نیز در اختیار دارد، به سادگی می‌تواند در لباس ادمین شبکه درآمده و ضدویروس و مکانیزم‌های محافظتی را غیرفعال نماید. لذا مانند گذشته توجه مدیران شبکه را به توصیه‌های زیر جلب می‌نماییم:

> **آنچه این باج‌افزار را خطرناک می‌کند، وجود یک نفوذگر انسانی در پشت آن است که از طریق پورت ریموت دسکتاپ و با استفاده از پسورد ادمین به سیستم‌های شبکه متصل می‌شود.**

۱- پورت ریموت‌دسکتاپ (RDP) را از بیرون از شبکه سازمان خود ببندید.

باز بودن پورت ریموت‌دسکتاپ (چه پورت پیش‌فرض ۳۳۸۹ و چه هر شماره پورت دیگری که برای آن تنظیم کرده‌اید) یکی از نقاط بسیار آسیب‌پذیر ویندوز و شبکه شما می‌باشد و به نفوذگران اجازه می‌دهد سر فرصت پسورد ادمین شبکه شما را کشف و به سادگی به آن وارد شوند.

متاسفانه علی‌رغم هشدارهای مکرر مراکز امنیت سایبری در این خصوص، همچنان شاهد سازمان‌هایی هستیم که با اطلاع ادمین یا به صورت ناخواسته، پورت ریموت باز داشته و از همین طریق هک شده‌اند.

۲- پشتیبان‌گیری منظم و مطمئن داشته باشید.

اساسی‌ترین مساله پس از هر نوع حمله بازگردانی سریع سرویس است. داشتن بکاپ منظم و مطمئن (که به سیستم متصل نباشد) یکی از مهمترین مولفه‌ها در دستیابی به این موضوع می‌باشد.

در همین راستا پیشنهاد می‌شود در سرورها، حجم اختصاص داده شده به بکاپ‌های داده‌بان پادویش را نیز حداقل تا ۱۵ درصد فضای درایو افزایش دهید.

۳- پسوردهای محکم و مناسب، در کنار به‌روزرسانی مداوم سیستم‌ها و نرم‌افزارها

امنیت یک زنجیر به هم پیوسته است که مقاومت آن به اندازه ضعیف‌ترین مولفه آن است. قوی‌ترین مکانیزم‌های امنیتی، نمی‌توانند از شما در برابر پسوردهای قابل حدس محافظت نمایند. به‌روز کردن سیستم‌ها و نرم‌افزارها، تعریف قواعد فایروالی مناسب در شبکه و عدم اجازه به انجام اتصالات غیرمجاز برحسب سیاست حداقل دسترسی، می‌تواند از بسیاری از آسیب‌ها جلوگیری نماید.

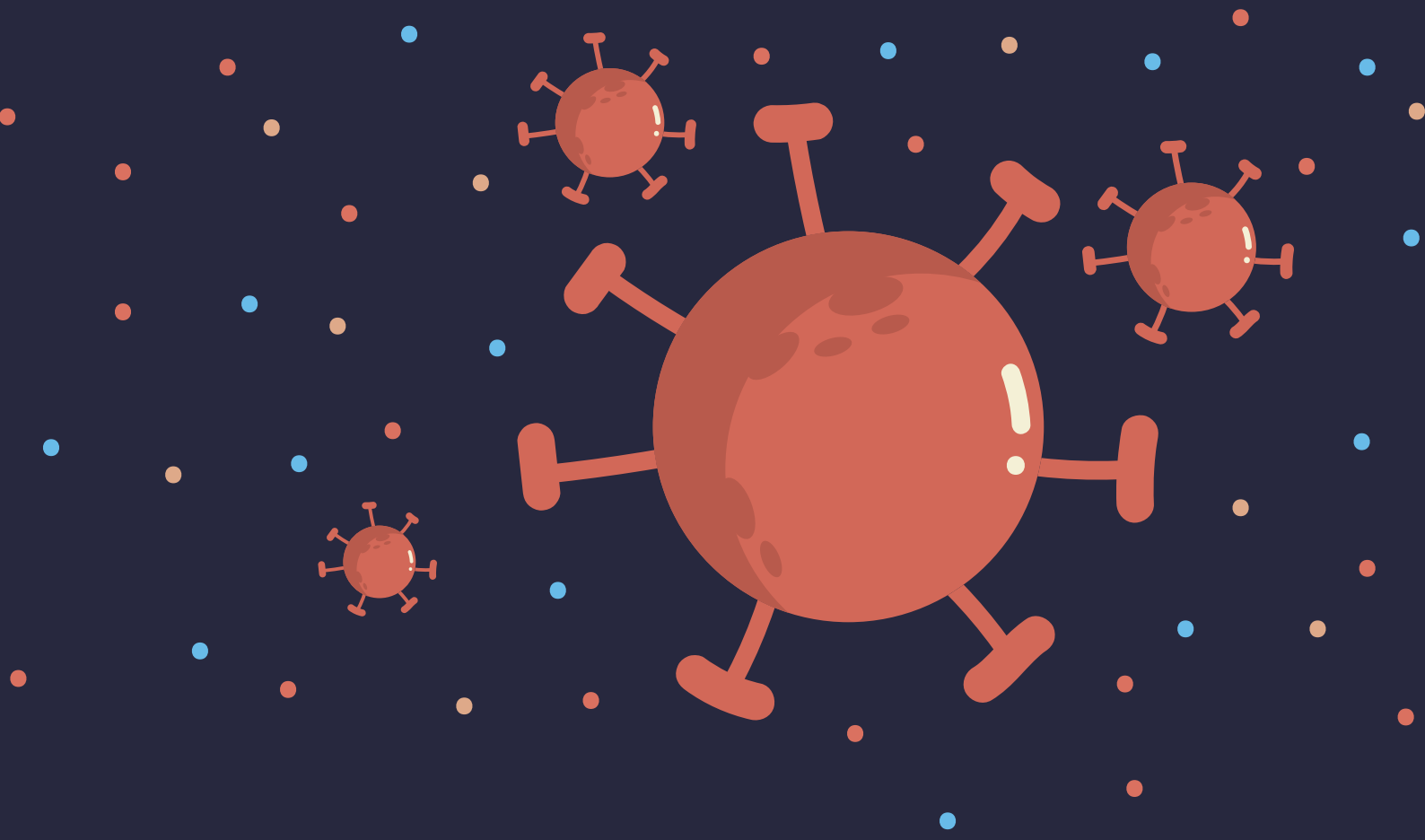
تهدیدها

تروجان HiddenAds

حتما برای شما هم پیش آمده که در زمان اوج مراجعه افراد به یک وب سایت پر بازدید مثل سایت‌های ثبت نام خودرو، به دلیل ترافیک بالای کاربران، موفق به ورود به سایت نشوید. به دلیل محدودیت و ظرفیت مشخص منابع موجود در شبکه، همواره به تعداد مشخصی از کاربران در یک زمان واحد سرویس داده می‌شود. در صورتی که تعداد مراجعان بیش از ظرفیت وب‌سایت باشد، سرعت لود شدن بسیار کند شده و بخشی از کاربران و یا حتی بیشتر آنها قادر به اتصال نخواهند بود.

برخی از بدافزارها با استفاده از این موضوع و به‌کارگیری حملات منع دسترسی به سرویس (Distributed Denial of Service) و با ارسال درخواست‌های بسیار زیاد به سایت هدف، روند سرویس‌دهی به مخاطبان آنها را مختل می‌کنند. البته این نوع از حملات تنها معطوف به وب‌سایت‌ها و گردانندگان آنها نمی‌شود. طبق گزارش آزمایشگاه تحلیل بدافزار پادویش، خانواده بدافزاری HiddenAds که مخصوص سیستم‌های اندوریدی است، با استفاده از همین تکنیک اقدام به ارسال مکرر درخواست به یک وب سایت مشخص می‌کند و همین امر موجب بالا رفتن ترافیک دریافتی توسط وب سایت مورد نظر شده و دسترسی به آن را محدود می‌کند. این بدافزار که از نوع تروجان است، با عنوان "به‌روزرسانی اندروید" از طریق وب‌سایت‌هایی که برای دانلود برنامه‌های اندرویدی هستند، در دسترس کاربران قرار می‌گیرد. بر خلاف ظاهر قانونی برنامه، روزانه حدود ۱۰ بار به سرور خود (C&C) متصل شده و دستورات مختلفی را دریافت و اجرا می‌کند.

> **بر خلاف ظاهر قانونی برنامه، روزانه حدود ۱۰ بار به سرور خود (C&C) متصل شده و دستورات مختلفی را دریافت و اجرا می‌کند.**



روند افزایش حملات سایبری با موضوع ویروس کرونا

با گذشت چندین ماه از همه‌گیری بیماری کووید ۱۹، بدافزارنویسان همچنان به فعایت‌های مخرب خود در زمینه انتشار بدافزار با موضوع ویروس کرونا مشغول هستند. حملات سایبری در ماه‌های اخیر عمدتا معطوف به سازمان‌های دولتی و مراکز پزشکی بوده است و حملات مشاهده شده بیشتر از نوع حملات باج افزاری و فیشینگ هستند. با این وجود، در هفته‌های اخیر موارد متعددی از تروجان‌های مخرب با موضوع ویروس کرونا گزارش شده است. طبق گزارش آزمایشگاه تحلیل بدافزار پادویش، بدافزار BAT. starter.cov یکی از تروجان‌هایی است که با سوءاستفاده از شیوع ویروس کرونا خود را به صورت برنامه‌ای کاربردی از طرف سازمان بهداشت جهانی معرفی و پس از نصب، سیستم را آلوده می‌کند. اصلی‌ترین نشانه‌های آلودگی به این بدافزار شامل موارد زیر هستند:

> **حملات سایبری در ماه‌های اخیر عمدتا معطوف به سازمان‌های دولتی و مراکز پزشکی بوده است و حملات مشاهده شده بیشتر از نوع حملات باج افزاری و فیشینگ هستند.**

- جایگزین شدن صفحه پیش‌زمینه ویندوز با زمینه کاملاً مشکی و عدم امکان تغییر آن
- تغییر در شکل مکان نمای ماوس
- بالا آمدن پنجره اخطار آلوده شدن سیستم و باز شدن مجدد آن پس از بستن

جهت پیشگیری از ورود این نوع بدافزارها به سیستم، پیشنهاد می‌شود از کلیک بر روی لینک‌های مشکوک خودداری نموده و فایل‌های ضمیمه ایمیل‌ها را قبل از اجرا، حتما پویش کنید. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت می‌کند.

باج افزار Lucy

استفاده روزافزون از گوشی‌های موبایل و ذخیره هر چه بیشتر اطلاعات شخصی و مهم کاربران، آنها را به هدفی مهم و پرسود برای سازندگان بدافزارها تبدیل کرده است. یکی از انواع بدافزارهای شایع و پرخطر، باج‌افزارها هستند که با گروگان گرفتن فایل‌های کاربر، درخواست باج (عموما به شکل ارزهای دیجیتال) می‌کنند که میزان باج درخواستی طی سال‌های گذشته به شکل چشم‌گیری افزایش یافته است. از آنجایی که سیستم عامل اندروید، رایج‌ترین نوع سیستم عامل مورد استفاده میان کاربران موبایل به شمار می‌رود، باج‌افزارهای اندرویدی بسیاری توسط بدافزارنویسان طراحی شده‌است. باج‌افزارها را می‌توان به انواع مختلفی طبقه‌بندی کرد اما بیشتر آنها در دو دسته کلی زیر جای می‌گیرند:

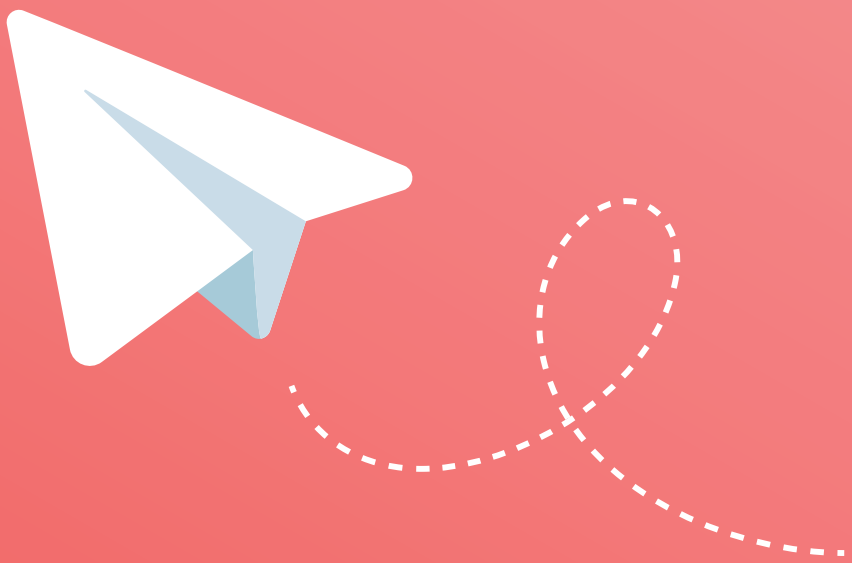
> **با دانلود و اجرای این بدافزار بر روی گوشی کاربر، تمامی فایل‌هایی که در قسمت‌های مختلف وجود دارند رمزگذاری و صفحه نمایش نیز قفل می‌شود.**

• باج‌افزارهای رمزگذار: این نوع باج‌افزارها فایل‌های کاربر را رمزگذاری و از دسترس او خارج می‌کنند که این روش معمولا برای سیستم‌های کامپیوتری به‌کار گرفته می‌شود.

• باج افزارهای قفل کننده: به جای رمز کردن فایل‌ها، با قفل کردن صفحه نمایش، از دسترسی کاربر به سیستم جلوگیری می‌کنند که روشی متداول میان باج‌افزارهای اندرویدی است.

به گزارش آزمایشگاه تحلیل بدافزار پادویش، باج افزار Lucy به عنوان نمونه‌ای از خانواده بدافزاری "Black Rose Lucy" مشاهده شده که به عنوان پخش کننده ویدیویی در دستگاه‌های اندرویدی معرفی می‌شود. با دانلود و اجرای این بدافزار بر روی گوشی کاربر، تمامی فایل‌هایی که در قسمت‌های مختلف وجود دارند رمزگذاری و صفحه نمایش نیز قفل می‌شود. در ادامه، پنجره‌ای در صفحه مرورگر باز می‌شود تا پیام سازندگان را به قربانی برساند. متن پیام ادعا می‌کند که از سوی پلیس فدرال ایالات متحده (FBI) است و قربانی را به داشتن محتوای مستهجن در دستگاه خود متهم می‌کند و در نهایت از کاربر می‌خواهد جریمه‌ای به مبلغ ۵۰۰ دلار بپردازد. در این شرایط، تنها راه پیش روی کاربر، پرداخت باج و دریافت کلیدی برای رمزگشایی فایل‌ها خواهد بود.

برای در امان ماندن از باج‌افزار Lucy و بدافزارهای مشابه، آنتی‌ویروس پادویش اندروید را نصب و اسکن آنتی‌ویروس را انجام دهید. آنتی‌ویروس پادویش این بدافزار را شناسایی و از سیستم حذف می‌کند.



بدافزار بازدید یاب تلگرام

بات تلگرام یک سرویس پیام‌رسان است که قابلیت‌های این نرم‌افزار را چند برابر می‌کند؛ از این رو به عنوان ابزاری محبوب و متداول میان کاربران شناخته می‌شود. بات‌ها برای انجام هدفی خاص مانند دانلود از یوتیوب، افزایش بازدید و لایک کانال، جستجوی تصاویر، فیلم و... مانند یک فرد حقیقی به فضای چت و کانال‌های عمومی اضافه می‌شوند. برخی از بدافزارها به کمک بات‌های تلگرامی به جاسوسی از تلفن‌های همراه کاربران و سرقت اطلاعات شخصی آنها می‌پردازند.

به گزارش آزمایشگاه تحلیل بدافزار پادویش، خانواده بدافزاری TeleRAT با بهره‌جویی از بات‌های تلگرامی، یک بات برای تحقق اهداف خود ایجاد و به واسطه دستورات ارسالی از سمت آن، اقدام به دزدی اطلاعات شخصی کاربر می‌کند. اطلاعاتی مانند تماس‌ها، پیامک‌های ارسالی و دریافتی، اطلاعات کاملی از گوشی و همچنین اقداماتی نظیر ضبط مکالمات، گرفتن عکس، باز کردن صفحات مختلف در تلگرام و ... را سرقت کرده و کاربران ایرانی را مورد هدف قرار می‌دهد. نام این برنامه که "بازدید یاب تلگرام" و از خانواده بدافزاری جاسوس افزارهاست، در بازارهای دانلود برنامه‌های اندرویدی مشاهده شده‌است.

از نسخه‌های غیررسمی برنامه‌ها استفاده نکنید. برنامه‌هایی مانند تلگرام و اینستاگرام نسخه‌های غیررسمی زیادی دارند و بیشتر آنها از طریق کانال‌های تلگرامی انتشار می‌یابند.

روش‌های پیشگیری از آلوده شدن گوشی

- از دانلود و نصب برنامه از منابع و مارکت‌های موبایلی نامعتبر خودداری کنید.
- هنگام نصب برنامه‌های موبایلی، به مجوزهای درخواستی دقت کنید.
- از فایل‌ها و اطلاعات ذخیره شده در گوشی پشتیبان‌گیری مداوم انجام دهید.

از نسخه‌های غیررسمی برنامه‌ها استفاده نکنید. برنامه‌هایی مانند تلگرام و اینستاگرام نسخه‌های غیررسمی زیادی دارند و بیشتر آنها از طریق کانال‌های تلگرامی انتشار می‌یابند. آنتی ویروس پادویش، این بدافزار را شناسایی و از سیستم شما محافظت 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