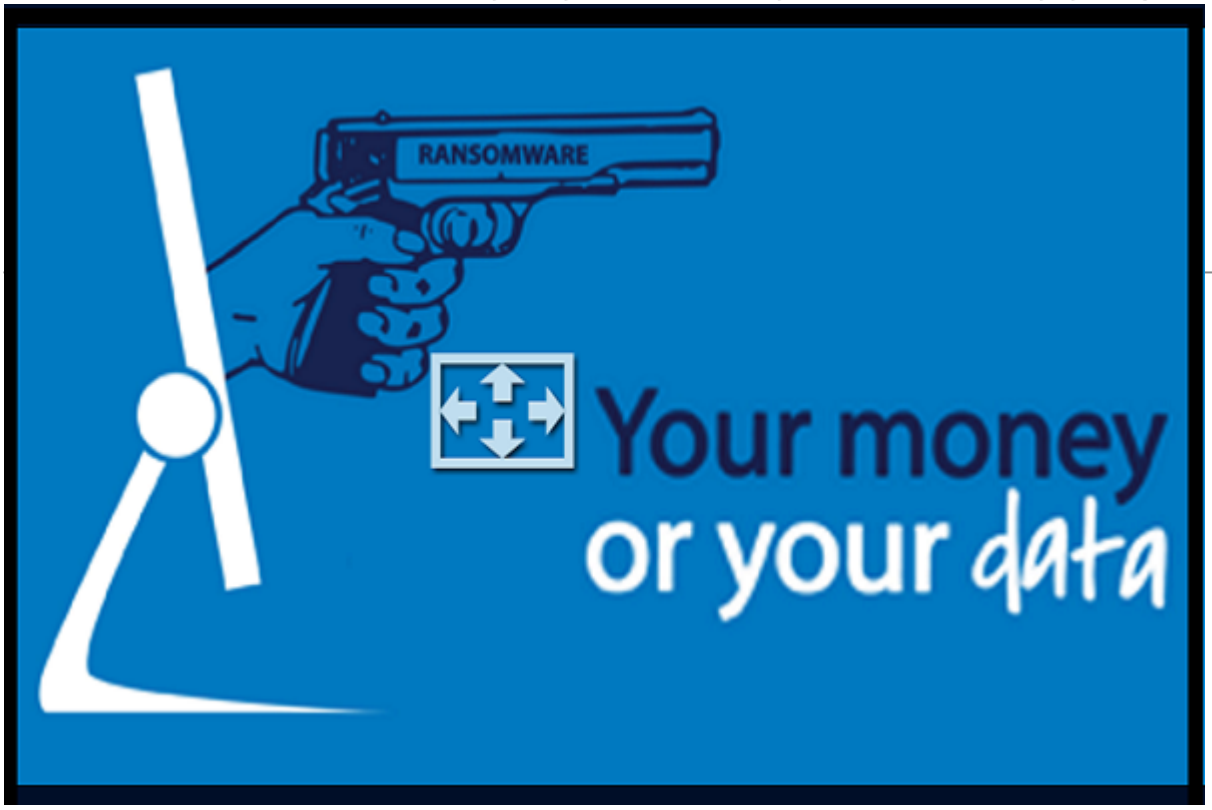
گونه جدید باج‌افزار Cerber یادگیری ماشینی را فریب می‌دهد



در یک دهه اخیر دو حوزه نرم‌افزار و سخت‌افزار پیشرفت‌های قابل ملاحظه‌ای را تجربه کرده‌اند. امروزه کامپیوترهای شخصی که از سوی کاربران مورد استفاده قرار می‌گیرند از قدرت محاسباتی بسیار بالایی بهره می‌برند. اگر از جنبه مثبت به این قضیه نگاه کنیم، مشاهده می‌کنیم این توان پردازشی بالا به توسعه‌دهندگان کمک کرده است الگوریتم‌ها و الگوهای برنامه‌نویسی که روزگاری پیاده‌سازی آن‌ها تنها با کامپیوترهای قدرتمند امکان‌پذیر بود را به راحتی طراحی کنند. اما از بعد منفی به هکرها کمک کرده است بدافزارهای پیچیده و شبکه‌ای از بات‌نت‌های مخرب را به وجود آورند.

شرکت‌های امنیتی برای حل اساسی این مشکل چاره را در آن دیدند که از هوش مصنوعی و الگوریتم‌های یادگیری ماشینی برای تحلیل الگوها و فعالیت‌های مخرب استفاده کنند. به طوری که حتا یک گام به جلو برداشتند و الگوهای رفتاری کاربران را نیز با هوش مصنوعی مورد تحلیل قرار دادند. در حالی که این تکنیک هنوز در مراحل اولیه خود به سر می‌برد اما تا حدودی موفق شده است با تحلیل پیشینه یکسری فعالیت‌های مخرب در مقابل یکسری از تهدیدات ایستادگی کند. این رویکرد باعث شده است تا هکرها منافع خود را در خطر ببینند و به دنبال دفاع باشند.

مطلب پیشنهادی

نسخه جدید که در فضای مجازی منتشر شده است
چگونه باج‌افزار سربر کاربران را با تخفیف فریب می‌دهد؟

در جدیدترین مورد کارشناسان امنیتی شرکت ترند میکرو گزارش کرده‌اند گونه جدیدی از باج‌افزار سربر را کشف کرده‌اند که در قالب ماژول‌های کوچک و مجزا از یکدیگر طراحی شده و کار می‌کنند. در ظاهر هر یک از این ماژول‌ها بی خطر به نظر می‌رسند. ماژول‌های فوق قادر هستند ابزارهای ضد بدافزاری که بر مبنای الگوریتم‌های یادگیری ماشینی تهدیدات را شناسایی می‌کنند را فریب دهند. گزارش‌های منتشر شده از سوی شرکت‌های امنیتی نشان می‌دهد هر زمان گونه جدیدی از این بدافزار منتشر می‌شود، یکسری ویژگی‌های جدید به آن اضافه می‌شود. ویژگی‌های جدید به این منظور افزوده می‌شوند تا به باج‌افزار فوق کمک کنند از سد سامانه‌های تشخیص بدافزاری

عبور کنند.

نکته قابل تعملی که در این بین وجود دارد، این است که توسعه‌دهندگان این باج‌افزار از نبوغ خاصی برخوردار هستند. به واسطه آن‌که این گروه از برنامه‌نویسان باید ویژگی‌های جدید را به گونه‌ای طراحی کنند که از حداقل کدها بهره برده اما در عین حال بالاترین کارایی را از خود نشان دهد. در شرایط عادی زمانی که نرم‌افزاری را طراحی می‌کنید با محدودیت حجم روبرو نیستید اما در دنیای هکری بدافزارها باید در کمترین اندازه خود طراحی شوند. مکانیزم مورد استفاده از سوی نسخه جدید به این گونه است که هر مرحله از عملیات خود را درون فایل جداگانه‌ای قرار داده و در مدت زمان اجرا این فایل‌ها را درون یک پردازه فعال در سیستم تزریق می‌کند. همین موضوع باعث شده است تا مکانیزم‌های تشخیص بدافزار قادر نباشند این بدافزار را شناسایی کنند.

باج‌افزار فوق چگونه کار می‌کند؟

همانند نگارش‌های قبلی، باج‌افزار سربر از طریق ایمیلی که در برگیرنده پیوندی به یک فایل آرشیو ذخیره شده در دراپ‌باکس است، برای قربانیان ارسال می‌شود. این حساب‌کاربری ساخته شده در دراپ‌باکس متعلق به هکرها است. درون این فایل فشرده سه فایل مجزا وجود دارد. یکی از این فایل‌ها یک فایل اسکریپتی ویژوال بیسیک است. فایل دوم یک کتابخانه پویا (dll) بوده و سومین فایل نیز یک فایل اجرایی است. فایل اسکریپت به منظور بارگذاری کتابخانه پویا مورد استفاده قرار می‌گیرد. در ادامه این کتابخانه پویا فایل اجرایی را فراخوانی کرده و آن‌را اجرا می‌کند. زمانی که باج‌افزار به طور کامل روی کامپیوتر قربانی نصب شد، در اولین گام وضعیت اجرا در محیط سندباکس را مورد ارزیابی قرار می‌دهد. اگر اطمینان حاصل کند که در یک محیط ایزوله شده به مرحله اجرا در نیامده است، بخش‌های باینری را درون پردازه‌های در حال اجرای سیستمی تزریق می‌کند.

ترندمیکرو در پستی که منتشر کرده آورده است: «هر چند رویکرد مورد استفاده از سوی نسخه جدید بدافزار سربر هوشمندانه است، اما این پتانسیل را ندارد تا به طور کامل از مکانیزم‌های ضدبدافزاری چند لایه عبور کند. بدافزار فوق در برابر دیگر مکانیزم‌های تشخیصی دارای نقاط ضعفی است. همین موضوع به ابزارهای تشخیص بدافزاری کمک می‌کند از طریق رویکردهای دیگری بدافزار فوق را شناسایی کنند. به طور مثال، اگر سامانه‌های تشخیصی به یک بسته آرشیو مشکوک شوند قادر خواهند بود از طریق روش‌های موجود محتوای درون این بسته‌ها را مورد بررسی قرار دهند. ابزارهایی که از راهکاری تشخیص مختلفی استفاده کرده و تنها به الگوریتم‌های یادگیری ماشینی وابسته نیستند، این توانایی را دارند تا در برابر چنین تهدیداتی از کاربران خود محافظت به عمل آورند.

تاریخ انتشار:

06 خرداد 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/7971/%DA%AF%D9%88%D9%86%D9%87-%D8%AC%D8%AF%DB%8C%D8%AF-%D8%A8%D8%A7%D8%AC%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-cerber-

%DB%8C%D8%A7%D8%AF%DA%AF%DB%8C%D8%B1%DB%8C-
%D9%85%D8%A7%D8%B4%DB%8C%D9%86%DB%8C-%D8%B1%D8%A7-
%D9%81%D8%B1%DB%8C%D8%A8-%D9%85%DB%8C%E2%80%8C%D8%AF%D9%87%D8%AF