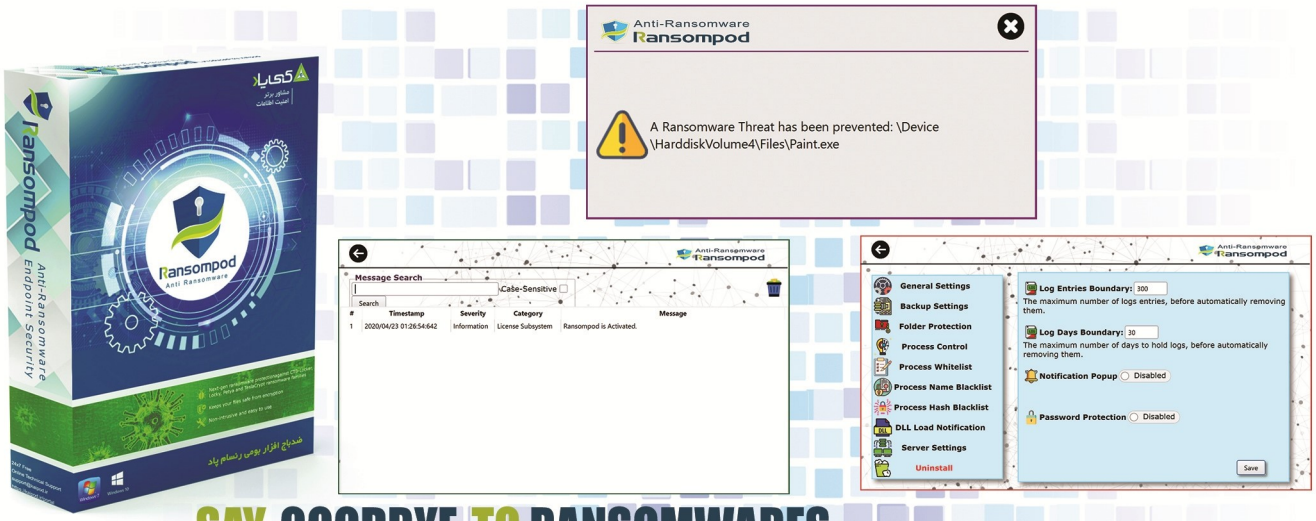
ضد باج‌افزار بومی شرکت پیشگامان کی‌پاد

ضد باج‌افزار رنسام‌پاد (Ransompod)

محصول ضد باج افزار بومی کی‌پاد بر اساس تکنیک ها و روش های هوشمند تولید شده است تا بدون نیاز به تحلیل کدها و داده های فایل اجرایی، مجازی سازی و شبیه سازی فایل اجرایی و موارد دیگر، قادر به تشخیص باج افزارها باشد. بدین ترتیب می توان از اغلب تکنیک ها و روش هایی که در محصولات آنتی ویروس سنتی برای مقابله با تهدیدات بکار می رود، فاصله داشت اما همچنان باج افزارها را به درستی تشخیص داد. در این راهکار روش های سنتی تحلیل پویا و راهبردهای هوشمند مبتنی بر تحلیل وقایع و دسترسی ها ترکیب شده اند، که نهایتا بدون نیاز به بانک اطلاعاتی امضاها و روش های سنتی تطبیق الگو، به نرخ تشخیص بسیار بالا در قبال گونه های مختلف باج افزار منجر می گردد.



SAY GOODBYE TO RANSOMWARES

باج‌افزار چیست؟

باج افزار گونه ای از بدافزارها است که از طرق مختلفی همچون ضمیمه های ایمیل، لینک های وب، آسیب پذیری نرم افزاری، رسانه های قابل حمل و ... به سیستم های قربانی راه پیدا می کند. باج افزارها همچون سایر بدافزارها هم به صورت Fileless و هم در قالب فایل های اجرایی معمولی وجود داشته و به فعالیت می پردازند. هدف اصلی باج افزار سلب دسترسی کاربر به منابع با ارزش در سیستم است که این امر معمولا به واسطه رمزنگاری فایل ها و منابع داده ای در آن سیستم انجام می شود. پس از سلب دسترسی به فایل ها معمولا از کاربران مبلغی به عنوان باج دریافت می شود تا به ازای آن مجددا امکان رمزگشایی فایل ها و دسترسی مجدد کاربر به آنها فراهم شود. البته در این شرایط هیچ تضمینی هم برای رمزگشایی و بازیابی فایل ها وجود ندارد!

فعالیت های معمول و روتین باج افزارها از قرار زیر هستند:

- حذف نسخه های پشتیبان در سیستم محلی
- حذف نسخه های پشتیبان در سیستم های پشتیبان گیری در شبکه
- حذف نقاط بازیابی سیستم عامل
- رمزنگاری فایل ها در سیستم محلی
- رمزنگاری فایل ها در اشتراک های شبکه (Network Share)
- رمزنگاری فایل ها در رسانه های قابل حمل
- انتشار از طریق اشتراک های شبکه
- انتشار از طریق رسانه های قابل حمل
- انتشار از طریق آسیب پذیری ها در سطح شبکه و آلوده سازی دیگر سیستم ها
- تخریب جدول آدرس دهی فایل ها در فایل سیستم (MFT)
- رمزنگاری یا تخریب سکتور MBR

برخی از قابلیت‌های ویژه رنسام‌پاد

از ویژگی های این محصول می توان به موارد زیر اشاره کرد:

- کنترل و نظارت بر اجرای پروسه ها از مبدا شاخه های موقتی (Temporary Folders)
- کنترل و نظارت بر اجرای پروسه ها از مبدا شاخه های کاربری نرم افزارها (AppData Folders)
- تهیه لیست سیاه جهت جلوگیری از اجرای پروسه های تعیین شده (Process Blacklisting)
- مکانیزم تشخیص بر اساس ظرف عسل (Honeypot)
- مکانیزم تشخیص هوشمند بر اساس تکرر دسترسی و تحلیل وقایع
- مکانیزم محافظت از سکتور MBR و فایل MFT
- مکانیزم محافظت از داده های پشتیبان (Volume Shadow Copies)
- مکانیزم محافظت از نقاط بازیابی سیستم عامل (System Restore Points)
- قابلیت کنترل و تشخیص یکپارچگی فایل ها بر اساس پسوندهای حساس تعیین شده
- قابلیت کنترل و تشخیص یکپارچگی فایل ها بر اساس شاخه مقصد تعیین شده
- قابلیت پشتیبان گیری خارجی از فایل ها بر اساس پسوندهای حساس تعیین شده
- قابلیت کنترل کامل بر چرخه داده در فایل ها بر اساس پسوندهای حساس تعیین شده
- قابلیت تعیین پوشه های حساس جهت جلوگیری از تغییرات در فایل ها
- قابلیت اطلاع از بارگذاری شدن کتابخانه های تعیین شده در پروسه های اجرا شونده
- پشتیبانی آنلاین و ثبت تیکت با ارسال لاگ ها به تیم پشتیبانی

معماری مورد پشتیبانی

- Ransompod Endpoint Security: 32-bit and 64-bit versions of Windows 7, 8, 8.1, 10
- Ransompod Server Security: 32-bit and 64-bit versions of Windows Server 2008, 2012, 2016, 2019
- Ransompod Enterprise Central Management Unit (CMU): Integrated & Centralized Management Web Console for Enterprise Networks, running on Linux OS