شهریور
۹۴

مجله

امنیت اطلاعات

شماره یازدهم

تحلیل بدافزار
معادله

Burn down chart چیست؟

در پشت صحنه‌ی تولید ضدویروس پادویش چه می‌گذرد؟

معیارهای شناخت یک ضدویروس خوب

به درخت نگاه کن...

قبل از اینکه شاخه‌هایش زیبایی نور را لمس کند؛

ریشه هایش تاریکی را لمس کرده...

گاه برای رسیدن به نور؛ باید از تاریکی‌ها گذر کرد...

در این شماره خواهید خواند:

تحلیل بدافزار معادله (Equation)

معرفی :

با انتشار خبر کشف بدافزار "معادله"، بررسی‌های اولیه‌ای صورت گرفت و مشخص شد طراحی و پیاده‌سازی این بدافزار نیز، هم‌چون موارد پیشرفته‌ی قبلی، ماژولار است. به طور کلی کدهای مربوط به بدافزار در قالب‌های متفاوتی از جمله فایل‌های اجرایی، درایور و پلاگین در سیستم اجرا می‌شود و تا کنون حدود پنج ماژول مختلف با نسخه‌های متفاوت کشف شده‌اند.

بررسی فایل‌های مرتبط با این بدافزار نشان می‌دهد که تاریخ پیاده‌سازی آن‌ها به اوایل سال ۲۰۰۸ میلادی بازمی‌گردد. هرچند تاریخ موجود در فایل‌های بسیاری از بدافزارها قابل اعتماد نیست، اما استفاده‌ی بدافزار از اکسپلویت معروفی که آسیب‌پذیری آن در نسخه‌های بعد از ویندوز xp برطرف شد به ما اطمینان می‌دهد که طراحی و پیاده‌سازی ماژول‌های بدافزار به زمانی قبل از به بازار آمدن نسخه‌های بعد از ویندوز xp بازمی‌گردد.

در قدم اول، دو ماژول EquationDrug و GrayFish به عنوان راه‌اندازهای اصلی ماژول‌های مراحل بعدی تشخیص داده شده و هدف تحلیل قرار گرفتند. این دو ماژول نه تنها از لحاظ عملکردی مشابه‌اند بلکه ساختار کد آن‌ها نیز بسیار به یکدیگر نزدیک است. علاوه براین استفاده از درایور و موتکسی با نام یکسان توسط این دو ماژول ارتباط نزدیک طراحان آن را تایید می‌کند. نکته‌ی جالب توجه این است که اکسپلویت ذکر شده نیز توسط هر دو ماژول با اندکی تفاوت به طور مشترک مورد استفاده قرارگرفته‌است! شاید ذکر این نکته جالب‌تر باشد که همین اکسپلویت در سال‌های بعد توسط بدافزار stuxnet نیز مورد استفاده قرارگرفت. به همین دلیل است که وجود ارتباط میان طراحان این دو بدافزار، stuxnet و Equation، دور از انتظار نیست. علاوه بر استفاده‌ی مشترک از این اکسپلویت، آن هم در زمانی قبل از انتشار این آسیب‌پذیری در سیستم عامل ویندوز، پی‌لودهای اجرا شده نیز اهدافی بسیار مشابه دارند.

اگرچه در روزهای اخیر انتشار خبر کشف این بدافزار کارشناسان زیادی را ترغیب به تحلیل این بدافزار کرده‌است، اما هنوز هیچ تحلیل دقیقی از این بدافزار منتشر نشده‌است.

در ادامه بخش‌هایی از تحلیل دقیق این دو ماژول ارایه می‌شود.

نحوه عملکرد:

۱ـ ماژول راه‌انداز EquationDrug

به طور خلاصه می‌توان گفت اجرای این ماژول در سیستم به عدم حضور برخی از دیواره‌های آتش وابسته‌است.

در صورت وجود هر یک از دیواره‌های آتش، EquationDrug فایل خود را قبل از اولین راه‌اندازی مجدد از بین برده و در غیر این صورت، بررسی می‌کند که دسترسی‌های لازم برای ساختن فایل و بارگذاری درایور را دارد یا خیر. در صورتی که دسترسی پایین‌تری داشته باشد با استفاده از آسیب پذیری که در win32k.sys وجود دارد، با بهره‌گیری از Privilege escalation exploit دسترسی‌های لازم را به دست می‌آورد و سپس ماژول‌های مراحل بعدی را دراپ کرده و راه‌اندازی و اجرا می‌کند.

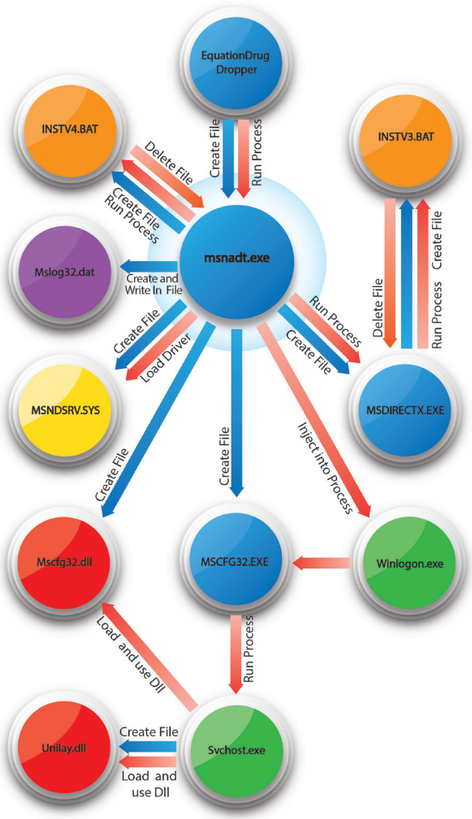
بعد از این عملیات و اجرای کلیه‌ی فایل‌های مورد نظر، در نهایت ماژول EquationDrug با دستور قبلی اقدام به از بین بردن فایل خود قبل از اولین راه‌اندازی مجدد می‌کند.

نکته‌ای که باید به آن اشاره کرد این است که کلیه‌ی کدهای مربوط به ماژول‌های مراحل بعدی و اطلاعاتی هم‌چون نام دیواره‌های آتش، همگی با الگوریتمی یکسان رمز شده و در بخش منابع(resources)، ماژول EquationDrug قرارگرفته‌اند. این کدها و اطلاعات در مراحل مختلف لود شده، رمزگشایی می‌شوند و مورد استفاده‌ی بدافزار قرار می‌گیرند.

علاوه بر این، این ماژول موتکسی با نام prkMtx را در سیستم می‌سازد.

۲ـ ماژول راه‌انداز GrayFish

به طور کلی این ماژول یکی از ماژول‌های راه‌انداز بدافزار است که نسبت به راه انداز دیگر گروه "معادله"، EquationDrug، از ساختاری



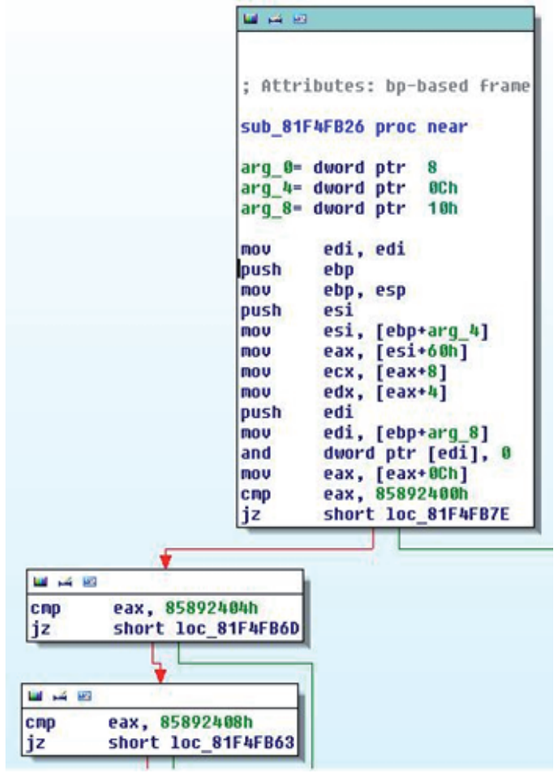
پیشرفته‌تر برخوردار است. با توجه به این‌که زمان کامپایل این ماژول به اوایل سال ۲۰۰۸ میلادی بازمی‌گردد می‌توان گفت تکنیک‌های به‌کار رفته در آن در زمان خود بسیار پیشرفته بوده و حتی برخی از آن‌ها برای اولین بار استفاده شده‌اند.

تقریبا تمامی رشته‌های مهم از قبیل نام APIها و Eventها، فایل‌ها و

ماژول‌های دیگر به صورت رمزشده نگه‌داری می‌شود. علاوه بر این به غیر از بخش انتهایی برنامه که بعد از انجام عملیات دراپ کردن و راه‌اندازی موفقیت‌آمیز درایورها فرا می‌رسد، کد سایر بخش‌ها غیرمبهم و تمیز است. در واقع در بخش ابتدایی برای دشوار شدن روال تحلیل، برنامه به‌جای استفاده از تکنیک‌های مبهم‌سازی و چندریختی، از تکنیک هوک بهره برده است. به طور دقیق‌تر می‌توان گفت برنامه‌نویس سعی کرده است برای جلوگیری از مشخص‌شدن روال کار، با استفاده از پیگیری APIهای استفاده شده، بخشی از کد یک درایور را در کرنل هوک کند. برای رسیدن به این هدف تابع IRP_MJ_DEVICE_CONTROL مربوط به درایورNull.sys انتخاب و هوک می‌شود. این هوک با بهره‌گیری از یک اکسپلویت معروف پیاده‌سازی شده است که توسط بدافزار stuxnet نیز مورد استفاده قرار گرفته بود (آسیب‌پذیری که در win32k.sys وجود دارد، همانند ماژول قبلی).
در این قسمت از توضیح دقیق روال کاری این اکسپلویت خودداری کرده‌ایم. نکته‌ی جالب توجه این است که علی‌رغم برطرف شدن این آسیب‌پذیری در ویندوزهای نسخه‌های بالاتر، بدافزار هم‌چنان تلاش می‌کند از اکسپلویت مذکور استفاده کند.
بعد از هوک کردن این تابع، کلیه‌ی فراخوانی‌ها به جای فراخوانی مستقیم APIها از طریق فراخوانی این تابع صورت می‌گیرد. برای مثال در زمان درخواست ساخت یک کلید رجیستری و یا نوشتن در آن، به جای استفاده از توابع معمول مثل RegCreateKey, RegSetValue به درایور Null.sys دستورات کنترلی ارسال می‌شود. بنابراین می‌توان گفت که کد فعال شده در این بخش هم‌چون یک API عمومی، (General API)، عمل می‌کند. به این معنی که با توجه به کنترل کد و ورودی‌های دریافتی تشخیص می‌دهد که باید چه اقدامی در سیستم صورت دهد.
با توجه به توضیحات داده شده به طور خلاصه روال کار بدافزار در این بخش در سه مرحله انجام می‌پذیرد.
مرحله‌ی اول: هوک کردن تابع ZwShutdownSystem
نتیجه: قرار گرفتن کد اولیه برای هوک کردن تابع IRP_MJ_DEVICE_CONTROL مربوط به درایورNull.sys
مرحله‌ی دوم: فراخوانی تقلبی تابع ZwShutdownSystem و اجرای کد اولیه
نتیجه: قرار گرفتن کد ثانویه به عنوان API عمومی در تابع مربوطه
مرحله‌ی سوم: فراخوانی متوالی API عمومی از طریق فراخوانی تقلبی تابع DeviceIoControl برای فایل با مسیر \\.\NUL
نتیجه: انجام کلیه‌ی فعالیت‌های راه‌انداز از این طریق
لازم به ذکر است که بدافزار از API عمومی خود برای مقاصد زیر استفاده می‌کند.

- عملیات خواندن و نوشتن کلیدهای رجیستری
- ساخت کلید رجیستری و پارامترهای آن
- خواندن و نوشتن در فایل
- ساخت فایل
- لود کردن درایورها در سیستم
- ساخت Thread

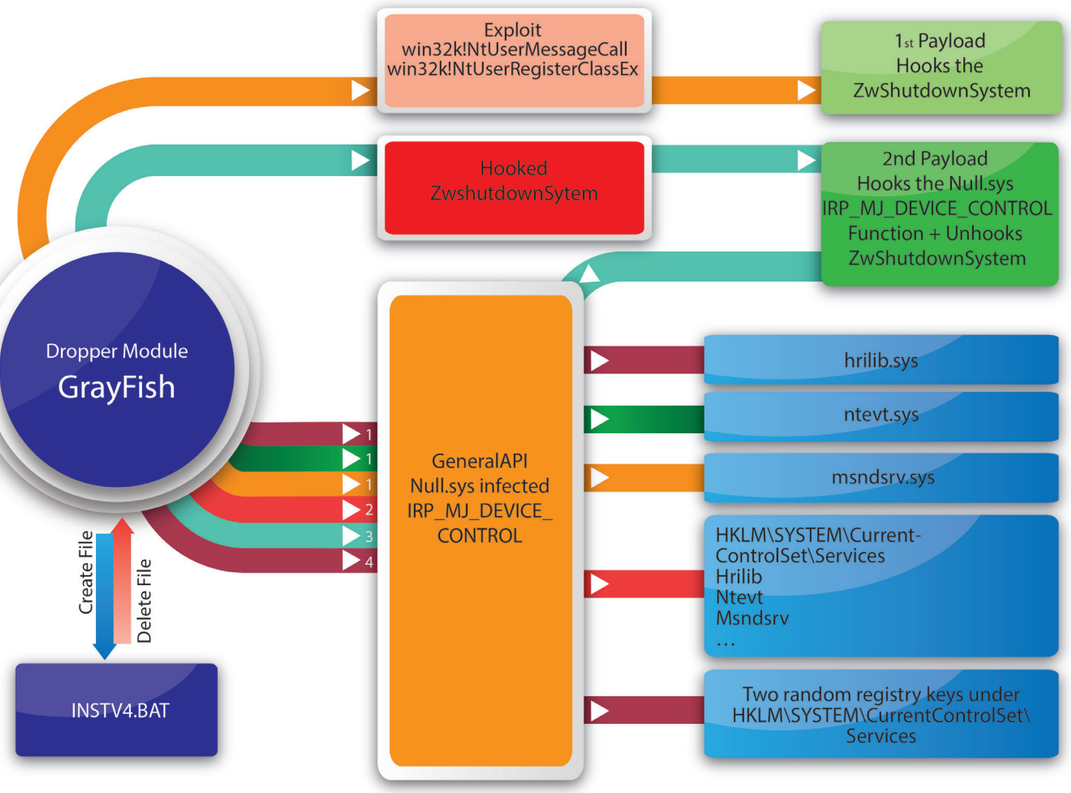
در شکل زیر می‌توانید نمایی از ابتدای دومین پی‌لود تابع را که به عنوان API عمومی عمل می‌کند مشاهده کنید. فلش‌های قرمز نمایشگر کدهای کنترلی‌ست که از سمت بخش کاربری به عنوان پارامتری کنترلی برای بخش کرنل ارسال شده و توسط بدافزار پشتیبانی می‌شود.



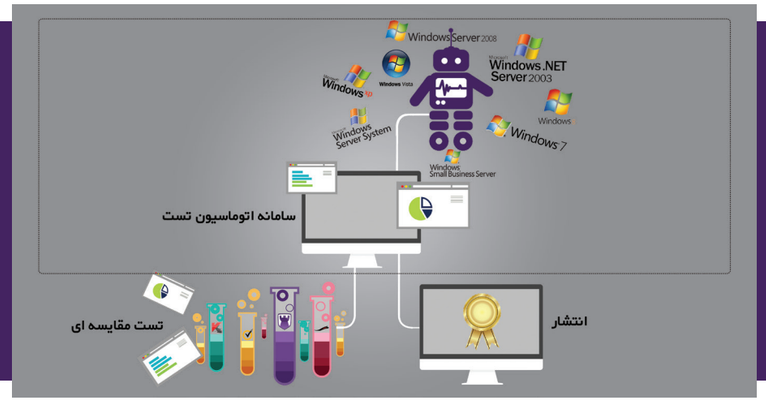
بعد از آماده شدن API عمومی، نوبت به ایجاد فایل‌های درایور بدافزار و لود کردن آن‌ها می‌رسد. همان‌طور که در شکل نمایش داده شده است سه درایور بدافزار به نام‌های Msndsrv، hrilib و Ntevt در مسیر SYSTEM32 ایجاد شده و در مرحله‌ی بعد راه‌اندازی می‌شوند.
توضیح این نکته ضروری به نظر می‌رسد که استفاده از نوع LegacyDriver در ماژول‌های درایور می‌تواند به قدیمی بودن زمان طراحی و پیاده‌سازی این ماژول اشاره داشته باشد؛ چرا که این درایورها وابسته به طراحی legacy Windows NT بوده و از نوع Non-Plug and Play Drivers می‌باشند.
در ادامه ماژول GrayFish از میان کلیدهای مربوط به سرویس‌های درایوری در رجیستری دو کلید را به‌صورت تصادفی انتخاب کرده و پلاگین‌های خود را که رمز شده است به عنوان پارامتر در آن‌ها ذخیره می‌کند. به نظر می‌رسد این پلاگین‌ها در مراحل بعدی توسط سایر ماژول‌ها مورد استفاده قرار گیرند.
یکی دیگر از موارد جالب دیده شده در روال این برنامه استفاده از تابع مستند نشده‌ی RtlImageDirectoryEntryToData برای دریافت جدول Import ماژول ntkrnlpa است. با استفاده از این تابع مستند نشده می‌توان اطلاعات متفاوتی را از یک فرمت PE لود شده در حافظه

استخراج کرده و خواند.
در انتها نیز فایل INSTV4.BAT در مسیر زیر ساخته می‌شود که حاوی دستور از بین بردن فایل اصلی برنامه است.

C:\Documents and Settings***\Local Settings\Temp



معیارهای شناخت یک ضدویروس خوب
(تست ضدویروس) بخش اول



در کشورهای مختلف دنیا سالانه مبالغ کلانی صرف تست نرم‌افزار می‌گردد. علاوه بر این، شرکت‌ها هزینه‌های زیادی را به جهت شکست نرم‌افزارها متقبل می‌شوند.
زمانی که یک برنامه، نیازمندی‌های مورد نظر را برآورده نکند با شکست روبه رو می‌شود. بدین ترتیب در هنگام تست به دنبال به دست آوردن یک برنامه‌ی ایده‌آل هستیم.
درمورد نرم‌افزار ضدویروس، علاوه بر انجام تست‌های فرایندی و عملکردی به عنوان یک نرم‌افزار بدون نقص در چرخه‌ی تولید، تست‌های دیگری نیز باید انجام شود.

تست ضدویروس

تست ضدویروس به دلیل دارا بودن نقش محافظت‌کننده، نحوه و میزان دسترسی‌ها به منابع سیستم و ماهیت نرم‌افزار ضدویروس بسیار حائز اهمیت می‌باشد. این تست‌ها شامل تست تاثیر ضدویروس بر کارایی سیستم، تست نرخ تشخیص ویروس، تست میزان خطای تشخیص ویروس، میزان تشخیص رفتاری ضدویروس برای ویروس‌های جدید، تست قابلیت پاک‌سازی سیستم آلوده، تست آنتی‌فیشینگ، تست‌های پویا و بلندمدت جهت بررسی عملکرد ضدویروس در محیطی نظیر دنیای واقعی و تست‌هایی از این قبیل می‌باشد.

تست کارایی

بخش عمده‌ای از تست‌ها پیرامون تست کارایی انجام می‌شود. کارایی ضدویروس در کنار ویژگی محافظتی یکی از نکات بسیار مهم برای اغلب کاربران می‌باشد. این ویژگی یکی از نکاتی است که هم کاربران خانگی و هم شرکت‌های حقوقی هنگام خرید محصول به آن توجه می‌کنند. هیچ کاربری به ضدویروس قدرتمندی که در عین قوی بودن تمامی منابع سیستم را مصرف نماید، نیاز ندارد زیرا در این شرایط کاربر دیگر قادر به انجام کار مورد نظر خود را با سیستم نخواهد بود.
اگرچه ارزیابی ویژگی محافظتی ضدویروس برای کاربران دشوار به نظر می‌رسد، درک این موضوع که سیستم‌عامل و یا سایر برنامه‌ها تا چه حد کند شده‌اند و یا کپی فایل ها یا بارگذاری صفحات وب چقدر آهسته‌تر شده است به راحتی امکان‌پذیر است. داشتن یک ضدویروس قابل اعتماد که تاثیر اندکی بر کارکرد سیستم داشته باشد، آرزوی هر کاربری است.

دقت تشخیص

در کنار تست کارایی این نکته نیز حائز اهمیت است که ضدویروس تا چه حد قادر است بدافزارهای موجود را شناسایی نماید. بالا بودن نرخ تشخیص برای امنیت کاربران بسیار مهم است. البته همیشه بالا بودن نرخ تشخیص نمی‌تواند ملاک خوب بودن یک ضدویروس باشد. در نتیجه تست میزان تشخیص نادرست ویروس در کنار تست نرخ تشخیص، دید کامل‌تری برای ارزیابی به ما می‌دهد. برای انجام این تست نیاز به یک مجموعه فایل می‌باشد. جمع‌آوری این مجموعه، خود نیازمند رعایت نکاتی است تا نتایج حاصل از تست قابل استناد باشد. از جمله مهم‌ترین نکاتی که باید به آن‌ها دقت داشت منبع نمونه‌ها، تنوع، جامع بودن، به روز بودن، بی طرفی، بازتابی از جهان واقعی بودن و هدف انجام تست می‌باشد.

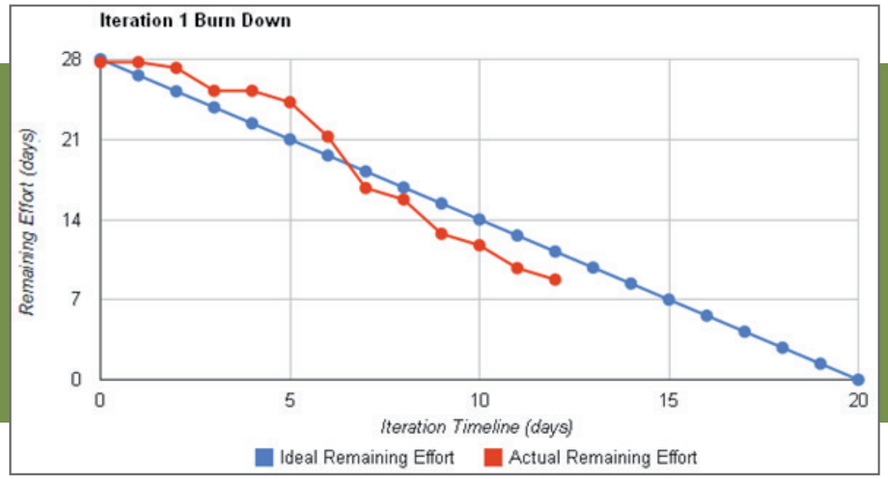
قدرت پاک‌سازی

پس از تشخیص آلودگی نوبت به پاک‌سازی سیستم می‌رسد. تشخیص آلودگی به تنهایی نمی‌تواند کمکی به کاربر نماید و سیستم باید از ویروس پاک شود تا امنیت کاربر تامین گردد.

خودکارسازی فرایند تست

تمامی این تست‌ها باید در محیط‌های مختلفی که کاربران با آن‌ها سروکار دارند شامل تمامی ویندوزها، سرویس‌پک‌های آن‌ها، سخت‌افزارهای مختلف و در کل شرایطی که یک کاربر با آن مواجه می‌شود، انجام گردد. انجام این حجم بالای تست و لزوم تکرار هر تست جهت جلوگیری از خطا، اهمیت استفاده از خودکارسازی تست‌ها را نشان می‌دهد. این سامانه خودکارسازی تست باید قابلیت تعریف تمامی این تست‌ها بر روی محصولات و محیط‌های اجرایی مختلف و همچنین دریافت نتیجه جهت تحلیل آن را داشته باشد.
در بخش‌های بعدی این سری مقالات فرایند انجام هر یک از تست‌های مطرح شده به تفصیل مورد بررسی قرار می‌گیرد.

Burn down chart چیست؟



توسعه محصولات نرم‌افزاری امری بسیار دشوار است و یکی از مهمترین دلایل آن، ناشناخته بودن زوایای مختلف محصول در حال توسعه است. بر این اساس و با توجه به اصل بقا و مزیت رقابتی کسب و کار، با دست خالی و بدون استفاده از ابزارهای کمکی نمی‌توان تصمیمات درستی اتخاذ کرد.
نمودار Burn down یکی از این ابزارهاست که به شما کمک می‌کند تا در زمان مناسب در مکان مناسب قرار گرفته و خود را اصلاح کنید.
Burn down chart یک نمودار گرافیکی برای نمایش وضعیت کارها برحسب زمان می‌باشد که از چپ به راست ترسیم شده و نمایش داده می‌شود. بیشترین استفاده و کاربرد این نمودار در پروژه‌های توسعه نرم‌افزار به روش چابک یا اسکرام می باشد. به عبارتی این نمودار وضعیت کلی فعالیت‌های جدید و درحال انجام را در هر اسپرینت با پیشرفت روزانه تیم در بازه‌ی زمانی مشخص شده برای هر اسپرینت، نشان می‌دهد.
با به‌روزرسانی وضعیت هر یک از فعالیت‌ها توسط تیم و SM (Scrum Master) این نمودار کارهای باقی مانده از هر اسپرینت را در هر روز نشان می‌دهد و نمایش آن در جلسات اسکرام به ارتباط بهتر اعضای تیم در جهت همگرا شدن با یکدیگر به منظور یک هدف مشترک، کمک می‌کند.
در اسکرام؛ هر پروژه به تعدادی اسپرینت به طول یک هفته تا یک ماه، هر اسپرینت به تعدادی Product Backlog Item یا PBI و هر PBI به تعدادی Task یا (Sprint Backlog Task)SBTتقسیم می‌شود.
این نمودار سرعت انجام کار لازم را برای رسیدن به هدف نهایی تیم که همان انتشار نسخه‌ی جدیدی از محصول می‌باشد، نشان می‌دهد که معمولا شامل چندین اسپرینت می‌شود.
Burn down chart یک ابزار تصویری مناسب در جهت پیگیری اهدافی نظیر بازگشت سرمایه (ROI) و همچنین نمایشی واضح از تاریخ اتمام پروژه می‌باشد. باکمک این نمودار PO(product owner) مالک محصول می‌تواند تعداد موارد کاری باقی مانده برای انتشار نسخه جدید را در هر اسپرینت به صورت جداگانه تخمین بزند. همچنین با یک بررسی و تحلیل درست از روند این نمودار می‌توان نیاز یا عدم نیاز به انجام کارهای دیگری در جهت رسیدن به اهداف کاری پروژه را نیز دریافت. این نمودار در عین حال نقش مهم و به سزایی در راستای آگاهی دادن به مدیران سطوح بالاتر پروژه دارد.
از این نمودار برای تخمین زمان خاتمه‌ی پروژه نیز استفاده می شود. به طور مثال اولین اسپرینت تیم با ۲۰۰ امتیاز[1] آغاز می‌شود اما در پایان اسپرینت، تیم ۱۵۰ امتیاز از کل فعالیت‌ها را انجام داده و در ابتدای کار نیز ۲۰ امتیاز دیگر به لیست کارهای تیم اضافه شده است. با در نظرگرفتن این اطلاعات از تمامی فعالیت‌های تیم می‌توان خطوط روند موارد تکمیل شده و روند موارد اضافه شده را در این نمودار ترسیم نمود. در اغلب نمودارها خط قرمز مشخص‌کننده‌ی روند موارد تکمیل شده و خط آبی مشخص‌کننده‌ی روند موارد اضافه شده است و هنگامی که این دو خط به هم می‌رسند در واقع زمان تخمینی پایان پروژه است.
به عبارتی دیگر می‌توان گفت که این نمودار به ما نشان می‌دهد که اگر فعالیت جدیدی به بک لاگ محصول اضافه نشود، پروژه در زمان مشخص شده، تکمیل و به اتمام می‌رسد. اما اگر فعالیت‌های جدیدی، با توجه به وضعیت سرعت انجام کار فعلی تیم، به پروژه اضافه گردد، این پروژه در یک یا دو اسپرینت بعد به پایان خواهد رسید. در نتیجه اگر به طور مداوم موارد جدید در بک لاگ محصول با سرعتی بیشتر از سرعت انجام، توسط تیم اضافه شود پروژه هیچ‌گاه به پایان نمی‌رسد و برعکس اگر سرعت تیم در انجام موارد بیشتر از سرعت اضافه شدن موارد جدید در بک لاگ محصول باشد پروژه سریع‌تر از آنچه برآورد شده به پایان خواهد رسید. در واقع مقایسه سرعت انجام فعالیت‌ها با حجم کارهای جدید (مجموع موارد اضافه شده) وضعیتی از پیشرفت پروژه را به ما نشان می‌دهد.

1. Point

خطر مضاعف برای گوشی‌های هوشمند اندروید

سیستم‌عامل اندروید با داشتن حدود ۲/۱ میلیون نرم‌افزار در گوگل پلی (فروشگاه برنامه‌ی گوگل)، یک میلیارد دستگاه فعال شده و ۵۰ میلیارد بار دانلود نرم‌افزار از گوگل پلی، محبوب‌ترین سیستم‌عامل گوشی به شمار می‌رود. گوشی‌های اندرویدی معمولا اطلاعاتی مانند داده‌های حساس نرم‌افزارهای مختلف (مانند نرم‌افزارهای بانک) ، پیام‌ها، مخاطبین، رمزهای عبور، ایمیل‌ها و اطلاعات شبکه‌های اجتماعی مختلف را ذخیره می‌کنند.

همه زندگی شما در گوشی شماست!

کاربران سیستم‌عامل اندروید غالبا نکات امنیتی را جدی نمی‌گیرند. استفاده از برنامه‌های دریافت شده از منابع مطمئن، عدم باز کردن ایمیل‌ها، پیام‌ها و صفحات مشکوک و خروج مطمئن از برنامه‌های حساس (مانند همراه‌بانک‌ها) پس از اتمام عملیات از این نکات امنیتی محسوب می‌شوند که معمولا جدی گرفته نمی‌شوند. عدم رعایت این موارد می‌تواند باعث آلودگی به بدافزار شود.

بدافزارهای موبایل در سه دسته کلی قرار می‌گیرند:

۱. بدافزارهای پیامکی

این نوع از بدافزار، با فرستادن یک پیام یا برقراری تماس، باعث می‌شود تا مبلغی از اعتبار حساب شما کسر شود. این پیام یا تماس می‌تواند با شماره‌های مخصوصی انجام شود تا مبلغ کسر شده به آن حساب انتقال داده شود.

۲. بدافزارهای درپشتی

این نوع بدافزار، بدون اطلاع شما اجازه‌ی دسترسی کامل به گوشی را از راه دور می‌دهند. یک نفوذگر می‌تواند از گوشی شما در جهت منافع خود استفاده کند و حتی برای شما دردسرساز نیز باشد.

۳. بدافزارهای جاسوسی

این نوع بدافزارها به دنبال ایمیل‌ها، پیام‌ها، مخاطبین، مکان شما و هرگونه اطلاعات دیگری هستند. حتی برخی نمونه‌ها توانایی ارسال عکس و صوت از میکروفون و دوربین گوشی هوشمند را دارا هستند. این بدافزارها، اطلاعات جمع‌آوری شده را به یک کامپیوتر مرکزی ارسال می‌کنند و به طرق مختلف از این اطلاعات استفاده می‌کنند.

نرم‌افزار نامطمئن از منبع نامطمئن؟!

در کشور ما، به دلایلی مانند تحریم، کاربران قادر نیستند همه نرم‌افزارهای خود را از منابع مطمئن دریافت کنند. از این رو، کاربران مجبور هستند نرم‌افزارهای مورد نیاز را از سایت‌هایی که توسط نهادهای مربوطه تأیید نشده‌اند، تهیه کنند. این امر موجب به خطر افتادن امنیت کاربران می‌شود. همچنین دریافت نرم‌افزارهای غیررایگان، از سایت‌هایی که این نرم‌افزارها را به صورت رایگان قرار می‌دهند نیز امنیت کاربران را با خطر مواجه می‌کند. این موارد، مخصوصا در کشور ما با توجه به شرایط خاص کشور، باید مورد تأمل بیشتری قرار گیرد.

راه چاره چیست؟

یکی از راه‌های اولیه‌ی مقابله با تهدیدات، استفاده از نرم‌افزار ضدویروس است. اما این نرم‌افزارها، به به‌روزرسانی مداوم نیاز دارند تا بتوانند حداکثر توان خود را در جهت امنیت به کار گیرند. از طرفی، با رشد سریع بدافزارهای موبایل، احتمال عدم تشخیص یک بدافزار توسط یک ضدویروس بالا می‌رود. به این دلیل، استفاده از ضدویروس به تنهایی قادر به برقراری امنیت کامل در گوشی هوشمند شما نیست.

سندباکس یک سیستم امنیتی است که در جهت شناسایی تهدیدات جدید و بررسی آن‌ها استفاده می‌شود. با استفاده از این سیستم، یک نرم‌افزار موبایل تحت یک سیستم به صورت خاص و ایزوله اجرا شده و گزارشی از عملکرد آن ارائه می‌شود. با مشاهده‌ی عملکرد نرم‌افزار، می‌توان به مشکوک بودن نرم‌افزار پی برد.

سندباکس اندرویدی جِورگ، اولین سندباکس ایرانی است و توسط محققان ایرانی به صورت کاملا بومی توسعه داده شده است. این سندباکس، با دارا بودن نسخه رایگان تحت وب، می‌تواند توسط افراد متخصص و غیرمتخصص مورد استفاده قرار گیرد.

سندباکس اندرویدی جِورگ، با قابلیت‌هایی مانند تحلیل ایستا، تحلیل پویا، تحلیل رفتار شبکه‌ای، تصویر صفحه‌نمایش از بدافزار در حال اجرا و جستجوی قوی در رشته‌های نرم‌افزار می‌تواند ابزاری بسیار کارآمد در جهت تحلیل و تشخیص بدافزارهای اندرویدی باشد.

برای استفاده از این سرویس و بارگذاری فایل‌های مشکوک خود، به آدرس زیر مراجعه کنید.

http://jevereg.amnpardaz.com/android

مجرمان اینترنتی در کمین کاربران نرم‌افزار WhatsApp

هیچ شکی وجود ندارد که نرم‌افزار WhatsApp یکی از محبوب‌ترین نرم‌افزارهای پیام‌رسان موبایلی است. در ماه گذشته این نرم‌افزار در نسخه‌ی افزونه‌ی مرورگر Chrome هم به بازار عرضه شد. مجرمان سایبری نیز از این خبر به عنوان یک روش کارآمد برای نفوذ به کاربران استفاده می‌کنند.

در هفته‌های اخیر پیغام‌های بسیاری در ارتباط با دانلود نسخه‌ی جدید نرم‌افزار WhatsApp به منظور فریب دادن کاربران در اینترنت مشاهده شده است که در حقیقت بسیاری از این پیغام‌ها آلوده به بدافزار بوده یا نسخه‌ای تقلبی از نرم‌افزار WhatsApp را دانلود می‌کند.

برای دانلود کردن نرم‌افزار WhatsApp لینک‌های دانلود تقلبی به زبان‌های مختلف در بسیاری از کشورها پخش شده است.

به طور مثال در عکس‌های زیر نمونه‌ای از لینک‌های دانلود تقلبی به زبان‌های برزیلی، اسپانیایی و عربی را می‌توانید مشاهده کنید:

از محصولات Mac استفاده می‌کنید؟ بدون آپدیت کردن آن؟ پس منتظر حمله هکرها باشید!

در پی کشف یک آسیب‌پذیری امنیتی، شرکت اپل برای اولین بار یک آپدیت امنیتی را برای کاربران خود تعبیه کرده است، که نیازی به تایید توسط کاربران ندارد.

این آسیب‌پذیری می‌تواند کنترل کامل سیستم‌عامل Mac را بدست بگیرد و به همین منظور این آپدیت برای آن منتشر شده است.

این آسیب‌پذیری بر روی بخش NTP (Network Time Protocol) و از نوع اجرای کد از راه دور (RCE) در سیستم‌عامل Mac یافته شد. اگر این پروتکل دچار سرریز بافر(Buffer Overflow) شود، آن‌گاه هکرها می‌توانند کدهای مخرب خود را بر روی سیستم قربانی اجرا کنند.

www.amnpardaz.com

در پشت صحنه‌ی تولید ضدویروس پادویش[1] چه می‌گذرد؟

ویروس نامی آشنا در حوزه‌ی کامپیوتر و به معنی برنامه‌های مخربی است که با انتشار روی رایانه‌ها برای کاربران ایجاد مزاحمت می‌کنند. برای اینکه رایانه‌مان به ویروس آلوده نشود، علاوه بر اجتناب از رفتارهای پرخطر، استفاده از یک ضدویروس مناسب و به روز یک راه حل منطقی است؛ نرم‌افزاری که با قرار گیری روی رایانه شما نقش پلیس را در برقراری امنیت اجرا می‌کند. ضدویروس به عنوان یک ابزار جلوگیری کننده از شیوع ویروس‌های رایانه‌ای وظیفه‌ی کشف، شناسایی و تعیین هویت و پاک‌سازی انواع ویروس‌ها را دارد. فناوری ساخت یک ضدویروس بسیار پیچیده است و این در حالی است که نرم‌افزاری که روی سیستم کاربران نصب می‌شود و آن را مشاهده می‌کنند تنها ۳۰٪ از کل کار انجام شده است و ۷۰٪ از کار در پشت صحنه اتفاق می‌افتد.

این بار در کشور به همت گروهی از متخصصان حوزه امنیت فناوری اطلاعات، ضدویروسی با نام پادویش (Padvish) تولید شده است. نام پادویش متشکل از دو بخش" پاد" به معنی ضد و "ویش" به معنی ویروس است. پادویش یک ضدویروس قابل رقابت با ضدویروس‌های رایج است که در طول شش سال تمام مراحل طراحی و پیاده‌سازی آن در شرکت نرم‌افزاری امن‌پرداز صورت گرفته است. این محصول به پشتوانه‌ی تکنولوژی شبکه‌ی ابر کاربران و تیم تحلیل بدافزار، قادر است به شناسایی جدیدترین بدافزارها در کمترین زمان ممکن بپردازد.

با ما همراه شوید تا با پشت صحنه این ضدویروس و دست‌اندرکاران آن آشنا شویم...

در پشت صحنه مقابله با ویروس در گروه پادویش اتفاقات مختلفی رخ می‌دهد. درست مشابه یک آزمایشگاه پزشکی، یک آزمایشگاه تحلیل ویروس وجود دارد که کارشناسان در آن به بررسی فایل‌ها، دسته‌بندی و تشخیص ویروس بودن آن‌ها می‌پردازند و از فایل‌های ویروسی یک کد شناسایی یکتا به نام امضا می‌گیرند که در واقع ضدویروس با استفاده از آن ویروس را شناسایی می‌کند. گاهی ممکن است به منظور مقابله با یک ویروس که مدام خود را تغییر می‌دهد عملیات کِشت ویروس انجام شود.

یکی دیگر از کارهای مهم، تولید پاک‌ساز برای یک ویروس است. ممکن است امکان حذف بخش آلوده از فایل آلوده به ویروس وجود داشته باشد که در این موارد فایل پاک‌سازی می‌شود اما مواردی نیز وجود دارد که در آن به دلایلی نمی‌توان بخش آلوده را از فایل پاک نمود که در این صورت ضدویروس با جلوگیری از اجرای آن بخش از فایل و به اصطلاح عقیم‌سازی فایل جلوی آلوده شدن سیستم را می‌گیرد.

ویروس‌ها برای جلوگیری از شناسایی شدن بی‌کارنمی‌نشینند و به روش‌های متنوعی جلوی شناسایی خود را می‌گیرند. از جمله این کارها پَک نمودن خود به شکلی است که نتوان محتوای اصلی آنها را متوجه شد. در این موارد لازم است در آزمایشگاه گروهی مسئول تولید آنپکرها باشند.

از آنجا که طبق آمارها سالانه حدود ۴۰۰ میلیون ویروس تولید می‌شود، بررسی انسانی همه این فایل‌ها ممکن نیست و در پشت صحنه ضدویروس پادویش اتوماسیون‌هایی وجود دارند که در حال کارکردن روی درصد بالایی از فایل‌ها به طور خودکار و ماشینی هستند و تنها موارد خاص به طور انسانی بررسی دقیق می‌شوند. در آزمایشگاه تحلیل بدافزار پادویش روزانه بیش از ۲۰۰,۰۰۰ فایل بررسی می‌شود و تعداد فایل‌هایی که به صورت غیر اتوماتیک(دستی) بررسی می‌شود تنها حدود ۵۰ مورد می‌باشد. یکی از دست آوردهای شرکت نرم‌افزاری امن‌پرداز در این حوزه سندباکس‌جِورگ[2] می‌باشد که با اجرای بدافزار روی یک محیط شبیه‌سازی شده ایزوله، همه فعالیت‌های فایل را رصد کرده و گزارش کاملی از آن را ارائه می‌کند که این گزارش در شناسایی و تحلیل فایل کاربرد دارد.

یکی دیگر از مهم‌ترین بخش‌های پشت صحنه، آزمایشگاه تست محصول است که مطابق با استانداردهای جهانی به تست محصول می‌پردازد. در این آزمایشگاه انواع ابزارهای تست خودکار تولید شده و از آنها به منظور کنترل کیفیت محصول نهایی استفاده می‌شود.

ضدویروس به دلیل اینکه در سطح سیستم‌عامل فعالیت می‌کند؛ اگر به هر دلیل در استفاده از منابع سیستم، عملکرد درست و بهینه‌ای نداشته باشد، موجب کندی سیستم و نارضایتی کاربر می‌شود. پرداختن به مباحث الگوریتمی در حوزه‌های مختلف به شکل حرفه‌ای از جمله وظایف مهمی است که گروه ضدویروس پادویش بر آن اهتمام ویژه‌ای دارد.

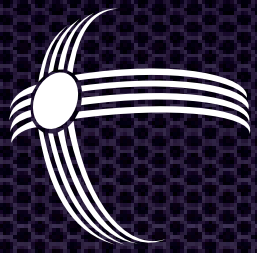
مدیریت حجم بالای فایل‌هایی که به عنوان نمونه‌های بدافزار نگه‌داری می‌شوند و تهیه بسته‌های به‌روزرسانی به طور مرتب و بی وقفه، نیازمند بستری مطمئن می‌باشد که مسایل فنی خاص خود را دارد.

رصد شبکه ابر کاربران به منظور تامین امنیت آن‌ها، یکی دیگر از وظایف مهم است تا بتوان ویروس‌های جدید را قبل از انتشار وسیع شناسایی کرده و به ورودی آزمایشگاه تحلیل بدافزار فرستاد تا به سرعت بتوان با آن‌ها مقابله کرد.

در آخر می‌توان گَفت بذر پادویش توانسته هم‌اکنون به نهالی نورس تبدیل شود و امید به آینده‌ای روشن داشته باشد. البته پادویش هم مانند هر ضدویروسی برای شکوفایی نیاز به اعتماد کاربران خود داشته و دارد.

1. http://www.padvish.com

2. http://jevereg.amnpardaz.com



شرکت نرم افزاری

امن پرداز

آدرس: تهران، خیابان ملاصدرا، خیابان
شیخ بهایی جنوبی، گرمسار غربی، پلاک ۷۶
تلفن:۴۳۹۱۲۰۰۰_۰۲۱ فکس:۴۳۹۱۲۸۰۰_۰۲۱
www.amnpardaz.com
info@amnpardaz.com