موتور هوشمند ضدویروس پاندا، REGIN را از مدت ها پیش شناسایی کرده بود...

برخی از موتورهای ضدویروس به سیستم های فدرتمند "پیش یابی" و "پیش شناسایی" کدهای مخرب مجهز هستند. این یعنی حتی ویروس های بسیار جدید، ناشناخته و ثبت نشده هم توسط آن ها قابل شناسایی و انسداد هستند.

نرم افزارهای شرکت پاندا سکیوریتی و موتور پیشرفته ضدبدافزار آن، دست کم از چهار ماژول پیش شناسایی ویروس ها که می توانند به صورت مکمل کار کنند، استفاده می کند :

Panda TruPrevent

Panda HDE

Panda IDS/IPS/HIPS

Panda Collective Intelligence (Based on Panda Cloud Security Technologies)

نرم افزارهای پاندا سکیوریتی در بسیاری از موارد، ویروس های جدید و خطرناک را حتی بدون جلب توجه مدیران شبکه (چه رسد به رسانه های بزرگ جهان) شناسایی، مسدود و قرنطینه می کنند (این فقط از طریق دسترسی به Detection Logهای برنامه ضدویروس و فقط برای مدیران شبکه قابل مشاهده است)

با توجه به این مسئله، بسیاری از بدافزارهای پیشرفته حتی به مرحله تحلیل، بررسی و اطلاع رسانی هم نمی رسند؛ زیرا...

-به صورت "خودکار" مسدود و قرنطینه می شوند

-کد پاکسازی آن ها به صورت "خودکار" تهیه می شود

-تمام مشتری های محصولات پاندا به صورت "خودکار" این کد پاکسازی را دریافت کرده و بروز رسانی می شوند.

نتیجه این که ضدویروس پاندا، بدافزارهای جدید و مهاجم مانندReginرا به صورت خودکار و پنهان کشف کرده، قبل از این که شرکت های دیگر بخواهند کشف آن را در بوق و کرنا کنند.

به هر حال تحقیقات و استعلام های شرکت ایمن رایانه نشان می دهد که تمام محصولات ضدبدافزار شرکت پاندا سکیوریتی، تمام گونه های جدید و قدیمی بدافزارReginرا شناسایی و پاکسازی می کنند و مدیران شبکه نباید نگرانی خاصی از بابت نفوذ یا فعالیت این ویروس داشته باشند؛ به ویژه در مراکزی که از ابزار Panda GateDefender eSeriesاستفاده می کنند، چون این ویروس ها قبل از نفوذ به درون شبکه، قابل شناسایی و حذف هستند.

بدافزار Regin در یک نگاه

خبرنامه ها

- خبرنامه شماره ۸۴ - ۲ آذر ماه ۱۳۹۳
- خبرنامه شماره ۸۳ - ۲۵ آبان ماه ۱۳۹۳
- خبرنامه شماره ۸۲ - ۱۸ آبان ماه ۱۳۹۳
- خبرنامه شماره ۸۱ - ۱۱ آبان ماه ۱۳۹۳
- خبرنامه شماره ۸۰ - ۴ آبان ماه ۱۳۹۳

پر بیننده ترین مطالب

- درباره فیلترشکن ها که امروزه خیلی هوادار دارد
- بررسی صفحه تقلبی فیس بوک زمانی که از ابزار freeGate استفاده می کنید
- فعالیت ویروس یا حسین
- نسخه آزمایشی ضدویروس 2014 پاندا منتشر شد به تکمیل پاندا 2014 کمک کنید و جایزه بگیرید
- اگر به فکر امنیت فایرفاکس خود هستید بخوانید...

آخرین اخبار

- موتور هوشمند ضدویروس پاندا، Regin را از مدت ها پیش شناسایی کرده بود...
- چگونه طعمه حملات فیشینگ نشویم... ؟!
- هشدار امنیتی در مورد هک شدن وب کم ها
- شروع همکاری تجاری شرکت پگاه سیستم و ایمن رایانه
- پاندا گلوبال پروتکشن 2015 ، نرم افزار برگزیده وب سایت ADSLZone
- فریب های اینترنتی و سوء استفاده از رویدادهای فیس بوکی ...
- هشدار امنیتی : کاربران آی فون در معرض "حمله بالماسکه"
- فناوری های نوین در دستان مجرمان سایبری...
- چگونه امنیت حساب کاربری Gmail را افزایش دهیم...؟
- هشدار امنیتی : دروپال در معرض هک گسترده اینترنتی قرار گرفت!
- ضدویروس های تحت مک پاندا از نسخه جدید OS X به خوبی پشتیبانی می کنند...
- شناسایی بیش از 20 میلیون گونه جدید از بدافزارها در سه ماهه سوم سال 2014
- مراقب ویروس های هالووین باشید... !
- هشدار امنیتی : بدافزار باجگیر The ICE Cyber Crime Center
- قابلیت " تأیید هویت دو مرحله ای" چیست و چگونه فعال می شود...؟
- تمامی مشترکین پاندا در مقابل تهدیدات ناشی از نقص امنیتی پاورپوینت در امان هستند!
- مشتریان بزرگ پاندا : مرکز پزشکی درمانی Infante D. Pedro ، کشور پرتغال
- شش نکته امنیتی مهم که برخی کاربران آنها را جدی نمی گیرند!

عنوان شناسایی شده توسط پاندا

Bck/Regin.A ، Generic Malware ، Trj/CI.A

توضیح: بدافزارهایی که توسط پاندا با نام های عمومی Generic Malwareو یاTrj/CI.Aشناسایی شده اند، در واقع توسط ماژول پیش شناسایی و پیش یابی ضدویروس پاندا کشف شده اند. این ها بدافزارهای فعالی هستند که به هر طریق توسط هرکدام از محصولات پاندا قابل کشف و پاکسازی هستند.

Generic Malwareو یا Trj/CI.Aطبقه بندی خاص و ویژه بدافزارها در محصولات پاندا هستند که ممکن است تا پایان زمان فعالیت یک ویروس خطرناک اطلاعات آن را در خود نگه دارند و باعث شوند که آن ویروس خاص به نام کلیGeneric Malware یاTrj/CI.Aشناسایی شوند. علاوه بر این بدافزارهای دارای نام های عمومی می توانند توسط هر کدام از ماژول های جانبی ضدویروس مانندPanda Cloud، Panda HDE Engineو ... به تنهایی شناسایی شوند.

نوع بدافزار:

بک دور / تروژان (RAT) / نرم افزار جاسوسی و سرقت اطلاعات/ APT/

MD5 Hashاصلی فایل مخرب:

2C8b9d2885543d7ade3cae98225e263b

تاریخ انتشار:

گونه های قدیمی از سال 1387 و قبل از آن، گونه های جدید و خطرناک از دوم آذر 1393 و قبل از آن.

توضیح: به دلیل امکان کشف خودکار ویروس ها توسط ماژول های پیش شناسایی موجود در برنامه های ضدویروس نمی توان تاریخ دقیق و رسمی برای کشف ویروس در نظر گرفت. بنابراین تاریخ کشف این بدافزار توسط پاندا، قبل از تاریخ های یاد شده می باشد

فعالیت های اصلی تخریبی :

-ایجاد آسیب پذیری در سیستم های رایانه ای با سیستم عامل ویندوز (شخصی یا سروری)

-نفوذ، مراقبت و سرقت اطلاعات طبقه بندی شده به صورت انبوه

چگونه از نفوذ و حملات ویروسReginمصون بمانیم؟

پاندا سکیوریتی به شما اطمینان می دهد که تمامی گونه های جدید و قدیمی ویروسReginتوسط موتور قدرتمند ضدویروس پاندا قابل شناسایی هستند؛ به شرطی که نکات زیر از طرف مدیران شبکه و کارکنان سازمانی رعایت گردد:

- بروز بودن کامل نرم افزار پاندا و اطمینان از عدم وجود مشکل در عملکرد آن بر روی "تمام" سرورها و سیستم هایسازمانی
تعریف دقیق و صحیح تمام سیاست های امنیت شبکه :

برای نمونه : کنترل تنظیمات شبکه
به روز رسانی نرم افزاری کاربری سازمان و مدیریت دائم اصلاحیه ها
مدیریت رمزهای عبور
تعریف دقیق و سخت گیرانه دسترسی کارکنان سازمانی در شبکه (بسیار مهم)
تعریف دقیق قوانین مربوط به امنیت پست الکترونیک
آموزش کارکنان سازمانی و اطلاع رسانی های دوره ای در حوزه امنیت شبکه
استفاده از ابزار مانیتورینگ اینترنت و نظارت بر دسترسی های اینترنتی کارکنان
پالایش محتویات اینترنتی ورودی به سازمان و موارد مهم دیگر

علاوه بر این می توانیددر شبکه و در رایانه های شخصی گاه به گاه از ابزارهای مکمل شناسایی و پاکسازی ویروس ها مثل برنامه رایگان و آنلاینPanda Cloud Cleanerاستفاده کنید. این برنامه ها با هر نوع برنامه امنیتی نصب شده در رایانه یا شبکه شما سازگار هستند و یک لایه مجزا و قدرتمند امنیتی بر روی تجهیزات رایانه ای شما ایجاد می کنند.

هم چنین می توانید برای افزایش ضریب امنیت شبکه و اطمینان از عدم آسیب پذیری آن از ابزار های مکمل مانند ابزارهای مدیریت یکپارچه تهدیدها (UTM)بر روی درگاه های اصلی اینترنت شبکه، ابزارهای مانیتورینگ و نظارت بر تجهیزات آی تی سازمان و یا

- مشتریان بزرگ پاندا، گروه صنعتی Tesco ، کشور پرتغال
- انتشاریک نسخه جعلی از برنامه ارتباطی "واتس اپ" در فضای اینترنت
- هشدار امنیتی مهم : انتشار بدافزار بانکی Com.ll ، پلت فرم اندروید
- مشتریان بزرگ پاندا : شرکت Data Solutions ، ایالات متحده آمریکا
- ویروس ایبولا... بهانه تازه کلاهبرداران اینترنتی برای ایجاد دلهره و نگرانی کاربران
- هفت میلیون حساب کاربری دراپ باکس در معرض خطر قرار دارند...
- هک شدن حساب های کاربری اسنپ چت و سرقت بیش از 200 هزار عکس خصوصی
- هک شدن حساب های کاربری اسنپ چت و انتشار عکس های غیراخلاقی
- امنیت کودکان و نوجوانان در اینترنت .... با بسته های نرم افزاری پاندا سکیوریتی
- داده های "سرگردان" ما در اینترنت، چقدر امن هستند؟
- مشتریان پاندا، شرکت BERNERS AB، کشور سوئد
- سرقت بیش از یک میلیون حساب کاربری در Viator
- همه چیز درباره Bash Bug؛ حفره امنیتی بزرگ در قلب فن آوری اطلاعات
- مشتریان بزرگ پاندا، شرکت خدمات امنیت آی تی AAAntivirus، ایالات متحده آمریکا
- کاربران اپل مراقب باشید... فریب تبلیغات دروغین را نخورید !
- نفوذ هکرها به سیستم پرداخت آنلاین Home Depot ، آمریکا
- کشف بی سابقه یک حفره امنیتی با بیشترین ریسک تخریبی ممکن
- اپل حریم خصوصی کاربران را امن تر می سازد !
- مشتریان بزرگ پاندا، مرکز پزشکی و درمانی Medistar، کشور آلمان
- پاندا سکیوریتی در نخستین نمایشگاه تخصصی امنیت سایبری ایران
- کشف یک آسیب پذیری خطرناک در چاپگرهای CANON
- مشتریان بزرگ پاندا : شرکت آکورو، کشور انگلستان
- دولت و بخش خصوصی در امن سازی فضای مجازی کشور به هم نیاز دارند
- دولت و بخش خصوصی در امن سازی فضای مجازی کشور به هم نیاز دارند
- با دایناسور آبی ملاقات کنید ... ابزار جدید فیس بوک برای افزایش امنیت حریم خصوصی شما
- بیش از 5 میلیون حساب کاربری جی میل هک شد ...
- مشتریان بزرگ پاندا : شرکت Delta Wines ، کشور هلند
- هجوم بی سابقه افزونه های ناخواسته اینترنتی
- چرا iCloud مقصر نیست؟
- مشتریان بزرگ پاندا : شرکت خدمات اینترنت iBurst ، آفریقای جنوبی
- هشدار جدی شرکت های امنیتی در مورد آسیب پذیری اندروید
- چرا "وایبر" ، هم محبوب است هم منفور؟!

ابزارهای کنترل و امنیت سرویس های پست الکترونیک استفاده کنید که شرکت پاندا سکیوریتی برای هرکدام از آن ها محصولات پیشرفته ای را در اختیار شما قرار می دهد.

نظرات

علی در تاریخ: چهارشنبه 05 آذر 1393 ، ساعت 10:09 ق ظ
با تشکر از اقدام به موقع شما.

3+

پاسخ دادن

مهران در تاریخ: چهارشنبه 05 آذر 1393 ، ساعت 12:09 ب ظ
به نظر من این ویروس رو سیمانتک گرفته فقط نفهمیدم این کسپرسکی این وسط چیکاره است؟
طبق معمول از دو سال پیش رصد می کرده می خندیده انگار!

2+

پاسخ دادن

بارگذاری مجدد فهرست نظرات

فید آر اس اس مربوط به نظرات این مطلب

ارسال نظر

نام

ایمیل

تغییرات به وجود آمده در نظرات را به من اطلاع دهید

ارسل