تکنولوژی ویروس‌کش eScan

فناوری‌های مبتنی بر محصولات امنیتی eScan

همان‌طور که قبل اشاره شد eScan یک ویروس‌کش پیشرفته و آنتی اسپم می‌باشد که می‌تواند با استفاده از تکنولوژی‌های منحصر به فرد و الگوریتمهای پیچیده و خلاقانه خاص ضد ویروس خود از سیستم‌ها در برابر تروجان‌ها، ابزارهای تبلیغاتی مزاحم، جاسوس افزارها، هرزنامه‌ها، هکر‌ها، فیشینگ‌ها و... محافظت کند. ما در این بخش مهم ترین تکنولوژی های ویروس کش eScan را به شما معرفی خواهیم کرد:

* **تکنولوژی PBAE**
* **تکنولوژی TSPM**
* **تکنولوژی NILP**
* **تکنولوژی MWL**
* **تکنولوژی DIRC**
* **تکنولوژی HIPS**

تکنولوژی PBAE

eScan آخرین فناوری PBAE (موتور تجزیه و تحلیل رفتار پیشگیرانه) را برای محافظت از کاربران ایجاد کرده است تا از سازمانها و کاربران در برابر حملات باج افزار در زمان واقعی محافظت کند.

تکنولوژی PBAE فعالیت کلیه پردازش ها را در سیستم رصد می‌نماید و به محض رو برو شدن با هرگونه فعالیت یا رفتار مشابه با یک باج افزار، یک پرچم قرمز بر روی آن ایجاد کرده و روند آن را مسدود می‌کند. درصورتی که سیستم آلوده در شبکه تلاش کند که به سیستم محافظت شده دسترسی پیدا کند و فایل‌های موجود در آن را رمزگذاری کند،PBAE بلافاصله آن را بی اعتبار نموده و تمامی ارتباطات شبکه‌ای با سیستم آلوده را قطع می‌کند.

PBAE با استفاده از هوش مصنوعی حملات باج افزار مانند Locky ، Zepto ، Crysis و موارد دیگر را مسدود می کند. علاوه بر این، با تجزیه و تحلیل داده های جمع آوری شده از طریق Cloud (ESN) قادر به شناسایی و کاهش هزاران حمله باج افزار به هر سیستمی می‌باشد.

تکنولوژی TSPM

با افزایش پیچیدگی حملات سایبری، بنگاه های اقتصادی میلیون ها دلار هزینه می کنند تا از جرایم اینترنتی جلوگیری کنند. با این حال ، به دلیل اقدامات نادرست امنیتی مانند استفاده از رمزهای ورود غیر حرفه‌ای ورود به سیستم، آسیب پذیرترین فرصت را برای مجرمان سایبری ایجاد می‌کنند. در چنین حالاتی، مجرمان سایبری برای به دست گرفتن کنترل شبکه حمله خواهند کرد.

برای تسهیل مدیریت متمرکز رایانه ها، سازمان ها RDP را پیاده سازی کرده تا از طریق LAN یا اینترنت به این سیستم ها دسترسی پیدا کنند. ‌به منظور محافظت از سیستم های فعال سرپرستان دیوار آتش را ایجاد می‌کنند تا RDP را برای سیستم هایی که می خواهند از راه دور مدیریت کنند، باز کند.

تکنولوژی TSPM آنتی‌ویروس eScan قادر است علاوه بر شناسایی حملات Brute Force به‌ صورت هوشمندانه آی.پی‌های مشکوک را بر روی پروتکلRDP شناسایی و مسدود نماید. در‌صورت وقوع حملاتRDP بلافاصله کلیه ارتباطات با سیستم و آی.پی حمله‌کننده را مسدود می‌نماید. احتمالا می‌دانید که هکر‌ها برای ایجاد بیشترین میزان خرابکاری به‌دنبال غیر‌فعال کردن مکانیزم‌ها و نرم‌افزار‌های امنیتی سیستم‌ها هستند، TSPM اینگونه وقایع را نیز شناسایی نموده و بلافاصله مدیران شبکه را مطلع می‌کند.

تکنولوژی NILP

NILP یک تکنولوژی ابداع شده توسط شرکت Micro World است که بر اساس اصول هوش مصنوعی کار می‌کند. این تکنولوژی رفتار کاربر را می آموزد هر ایمیل را مطابق با الگو‌های رفتاری کاربر تجزیه و تحلیل می‌کند سپس با یک تصمیم آگاهانه به شناسایی و طبقه بندی نامه‌ها که معمولا ایمیل یا هرزنامه هستند می‌پردازد. NILP یک مکانیزم یادگیری متفاوت است که از سرور‌های شرکت Micro World تغذیه می‌شود.

تکنولوژی MWL

فناوری MicroWorld Winsock Layer یک فناوری انقلابی است که در لایه Winsock سیستم عامل قرار دارد و تمام ترافیک ورودی و خروجی اینترنت را اسکن و محتوای آلوده را مورد بررسی قرار می‌دهد. به این شکل که بر‌خلاف دیگر آنتی‌ویروس‌های موجود این آنتی‌ویروس تروجان‌ها و حمله‌های ویروسی را در لایه Winsock تشخیص می‌دهد. پس درصورت تشخیص ویروس و تروجان از ورود آن‌ها به لایه سیستم ممانعت به‌ عمل می‌آورد، در غیر این صورت داده‌ها را عبور می‌دهد.

از نظر فنی ، MWL بالاتر از لایه WinSock قرار می گیرد و به عنوان "دروازه بان شفاف" در لایه WinSock سیستم عامل عمل می کند. تمام بسته های داده ای که از پورت های TCP / IP مختلف وارد می شوند ، جمع می شوند. سپس ترافیک ایمیل و وب ، ترافیک FTP و ICQ را بهمراه تمام پیوستها رمزگشایی کرده و آنها را از طریق فیلترهای متعددی مانند فیلترهای ویروس ، فیلترهای محتوا ، فیلترهای پیوست و غیره عبور می دهد. این فیلترها اعتبار محتوای فایل را بررسی می کنند و اعلان های پویا را صادر می کنند .

فناوری MWL بر کلیه داده های ورودی به اینترنت و نظارت بر آنها نظارت دارد و در نتیجه به آن اجازه می دهد بدون تداخل با برنامه ها ، آنها را پردازش کند. امکانات فشرده سازی و فشرده سازی دینامیکی جریان داده ، بین اینترنت و رایانه شما به منظور حداکثر استفاده از پهنای باند موثر ، توسط MWL فراهم شده است.

تکنولوژی DIRC

اغلب افراد و سازمان‌ها از ایمیل برای مکاتبات خود استفاده می‌کنند. بنابراین بیشتر مردم از پر شدن صندوق ورودی ایمیل‌های خود از ایمیل‌های نا‌خواسته و یا اسپم‌ها ناراضی هستند. مانند سایت‌های رباینده اطلاعات حیاتی، سایت‌های حاوی ویروس و نرم‌افزار‌های مخرب دیگر. پس این برای کاربران ضروری است که بتوانند تشخیص دهند ایمیلی که دریافت کرده‌اند معتبر و از یک منبع قابل اعتماد است یا خیر. اعتبار یک فرستنده ایمیل بستگی به معیار‌هایی دارد مانند تعداد آدرس‌های نا‌معتبری که فرستنده ایمیل به آن‌ها ایمیل فرستاده است، یا تعداد شکایاتی که از فرستنده اسپم انجام شده است و یا آی.پی آدرس‌های فرستنده ایمیل.

 این مفهوم اعتبار‌سنجی مبتنی بر آی.پی فرستنده نام دارد و از آن برای تعیین اعتبار از یک آی.پی آدرس بر اساس آنچه در گذشته فرستاده شده است استفاده می‌شود.این رویکرد به سهم خود معایب و مضراتی هم دارد. اگر یک سازمان از خدمات بازاریابی برای بازاریابی محصولات خود استفاده کند امکان دارد آی.پی آدرس‌های خود را با سازمان‌های دیگری که از همان خدمات استفاده می‌کنند، به اشتراک بگذارد. بنابراین اگر یکی از سازمان‌ها درگیر اسپم‌ها و فایل‌های مخرب باشد، همه سازمان‌های مربوطه دیگر نیز دارای همان اعتبار آی.پی خواهند بود و با آن‌ها یکسان برخورد می‌شود. علاوه بر این اگر یکی از سازمان‌ها آی.پی خود را تغییر دهد، اعتبار آی.پی آن سازمان به آی.پی جدید آن بستگی خواهد داشت.اما در صورتی که سازمان از یک نام دامنه واقعی (Domain Name) به جای یک آی.پی آدرس استفاده کند اعتبار آن مستقل از خود کامپیوتر یا جا و مکان آن خواهد بود. این مفهوم تعیین اعتبار فرستنده مبتنی بر دامنه (Domain) نامیده می‌شود. اما بیشتر سازمان‌ها از هر دو قابلیت اعتبار‌سنجی بر مبنای آی.پی و بر مبنای دامنه (Domain) استفاده می‌کنند. بنابراین، ای‌اسکن از تکنولوژی DIRC برای بلاک کردن اسپم‌ها استفاده می‌کند.

مزایای DIRC

* DIRC اعتبار سازمان را از وابسته بودن بهIP آدرس یک کامپیوتر یاDomain رها می سازد.
* مانع از رسیدن هرزنامه به صندوق دریافت ایمیلهای کاربر میشود .

تکنولوژی HIPS

معمولا آنتی‌ویروس‌ها تنها زمانی تروجان و ویروس را تشخیص می‌دهند که سیستم آلوده شده است. اکثریت این برنامه‌ها روشی بر دیتابیس تعریف شده را استفاده می‌کنند. این به این معناست که آنتی‌ویروس‌ها فقط تروجان‌ها و ویروس‌هایی را تشخیص می‌دهند که آن‌ها را از قبل بشناسند. این روش هنگامی که یک برنامه مخرب جدید منتشر می‌شود باعث بروز مشکلاتی در سیستم می‌گردد.

 HIPS کلیه فعالیت‌های شبکه را بر روی سیستم کنترل می کند. این فناوری به شما در شناسایی جاسوس افزار یا Trojan بر روی سیستم کمک می کند. فناوری HIPS نه تنها در مورد هرگونه نفوذ سیستم هشدار می دهد، بلکه از آن ممانعت می‌کند.

فناوری HIPS از تشخیص مبتنی بر امضا و الگوریتم پیشرفته آنتی ویروس اکتشافی استفاده می کند. همچنین می توانید خط مشی هایی را تعیین کند که رفتار سیستم عامل ها یا برنامه ها را مشخص می کند. حملاتی که HIPS در برابر آنها محافظت می کند شامل ویروس ها، اسپم ها، جاسوس افزارها، کرم ها، تروجان ها، keylogger ها، ربات ها است.

**Proactive Behavioral Analysis Engine (PBAE) Technology**

We had predicted in our threat predictions that Ransomware will be a major threat in the year 2016. This year has seen an unprecedented growth of more than 172% rise in ransomware attacks and many corporate and government organizations have fallen prey to ransomware attacks. Though widely not reported, it has cost millions of dollars to many organizations across the world. If you want to know what is Ransomware, here are some resources that will help you to safeguard against this type of attack

**eScan Launches new TSPM Technology to block RDP hacking attacks**

With the growing complexity of cyber-attacks, enterprises are spending millions to avoid cyber-crime. However, due to bad security practices such as usage of elementary passwords for system access creates most vulnerable opportunity for cyber criminals. In such scenarios cyber criminals use brute force attack to take control of network. Based on “National Exposure Index” report by Rapid7, 73% of Indian RDP servers are exposed to bruteforce attacks, and ranks 18th on the Global Index.

**MicroWorld Winsock Layer (MWL) Technology**

The MicroWorld Winsock Layer technology is a revolutionary technology that resides on the Winsock Layer of the operating system and scans all the incoming and outgoing traffic from the Internet and checks for any security violating content. If the data packet is clean it is passed or else it is removed before it reaches the application layer.

**Domain & IP Reputation Check**

The Domain & IP Reputation Check technology verifies the credibility of Web domains by tracking any indication of suspicious activities on the web page. This technology also verifies the integrity of the IP address by comparing it with a list of known email senders and by using a dynamic service that assesses email senders reputation in real-time. Emails received from domains with malicious activities are not accepted.

**Non Intrusive Learning Pattern (NILP) Technology**

NILP works on the basis of Artificial Intelligence where in, it learns user's behavior and then takes an informed decision in the background and help identify and classify mails on behalf of the users whether the mails are spam or ham.