به نام خداوند یکتا

مستند

الگوهای شناسایی بدافزار

آنتی‌ویروس eScan

(eScan AV Signatures)

تاریخ انتشار: خردادماه ۱۳۹۵

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

فهـرسـت

۱- الگوهای شناسایی بدافزار توسط آنتی‌ویروس ۳
۲- نحوه‌ی ایجاد الگوهای شناسایی بدافزار ۴

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

۱- الگوهای شناسایی بدافزار توسط آنتی‌ویروس

این مستند، درمورد الگوهای شناسایی بدافزار (امضاهای ویروس) و نحوه‌ی دانلود آن‌ها توسط آنتی‌ویروس eScan به منظور مقابله با آخرین تهدیدهای مبتنی بر بدافزار ارائه شده است. الگوهای شناسایی بدافزار (امضاهای ویروس) هسته‌ی اصلی هر آنتی‌ویروس محسوب می‌شوند و بدون این ابزار، آنتی‌ویروس قادر به شناسایی و حذف بدافزارها نمی‌باشد. در واقع، می‌توان نقش الگوهای شناسایی بدافزار (امضاهای ویروس) را به مثابه گلوله تفنگ در عملکرد بیان نمود. به منظور به‌روزرسانی آنتی ویروس، باید الگوهای شناسایی بدافزار (امضاهای ویروس) از وب‌گاه تولیدکننده آن دانلود و پایگاه داده‌ی آن به‌روز گردد. به طور متداول، آنتی‌ویروس‌ها به طور خودکار، فرآیند دانلود و به‌روزرسانی الگوهای شناسایی بدافزار (امضاهای ویروس) را عملیاتی می‌نمایند.

در این مستند، نحوه‌ی دانلود الگوهای شناسایی بدافزار (امضاهای ویروس) توسط آنتی‌ویروس eScan، موقعیت دانلود آن‌ها توسط آنتی‌ویروس، نحوه‌ی به‌روزرسانی محصولات نسخه‌ی خانگی و دفاتر کوچک (SOHO) و نیز، نحوه‌ی به‌روزرسانی محصولات نسخه‌ی تحت شبکه، سازمانی و توزیع الگوهای شناسایی بدافزار (امضاهای ویروس) تحت شبکه ارائه خواهد شد.

در آغاز باید تعریف الگوهای شناسایی بدافزار (امضاهای ویروس) بیان شود. الگوهای شناسایی بدافزار (امضاهای ویروس)، رشته‌های باینری و به‌روزرسانی‌های ارائه شده توسط تولیدکنندگان آنتی‌ویروس به منظور مقابله با آخرین تهدیدهای مبتنی بر بدافزار می‌باشند. هر بار که پایگاه داده‌ی الگوهای شناسایی بدافزار (امضاهای ویروس) دانلود و به‌روز گردد، بر اساس آن‌ها، تهدیدهای منطبق با الگوی تعریف شده، شناسایی و توسط موتور آنتی‌ویروس حذف می‌گردند. پیاده‌سازی این مقوله، نیاز به تلاش فراوان و آزمایش‌های متنوع در جهت ایجاد الگوهای شناسایی بدافزار (امضاهای ویروس) دارد.

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

۲- نحوه‌ی ایجاد الگوهای شناسایی بدافزار

هر بار که نمونه فایل‌های حاوی بدافزار در لابراتوار تحلیل بدافزار eScan دریافت می‌شود، بر اساس چندین رویه، ایجاد الگوهای شناسایی بدافزار عملیاتی می‌گردد. تحلیلگران بدافزار شرکت eScan با انجام آزمون‌های استاتیک و پویا در زمان اجرای نمونه فایل‌های حاوی بدافزار، رفتار سیستم را تجزیه و تحلیل می‌نمایند. بر اساس اطلاعات گردآوری شده از این فرآیند، الگوهای شناسایی بدافزار (امضاهای ویروس) ایجاد و در گام بعدی آزمون‌های میزان شناسایی و تشخیص نادرست به عنوان بدافزار (False Positive) انجام شده و در نهایت پس از طی این گام، الگوهای شناسایی بدافزار انتشار می‌یابند.

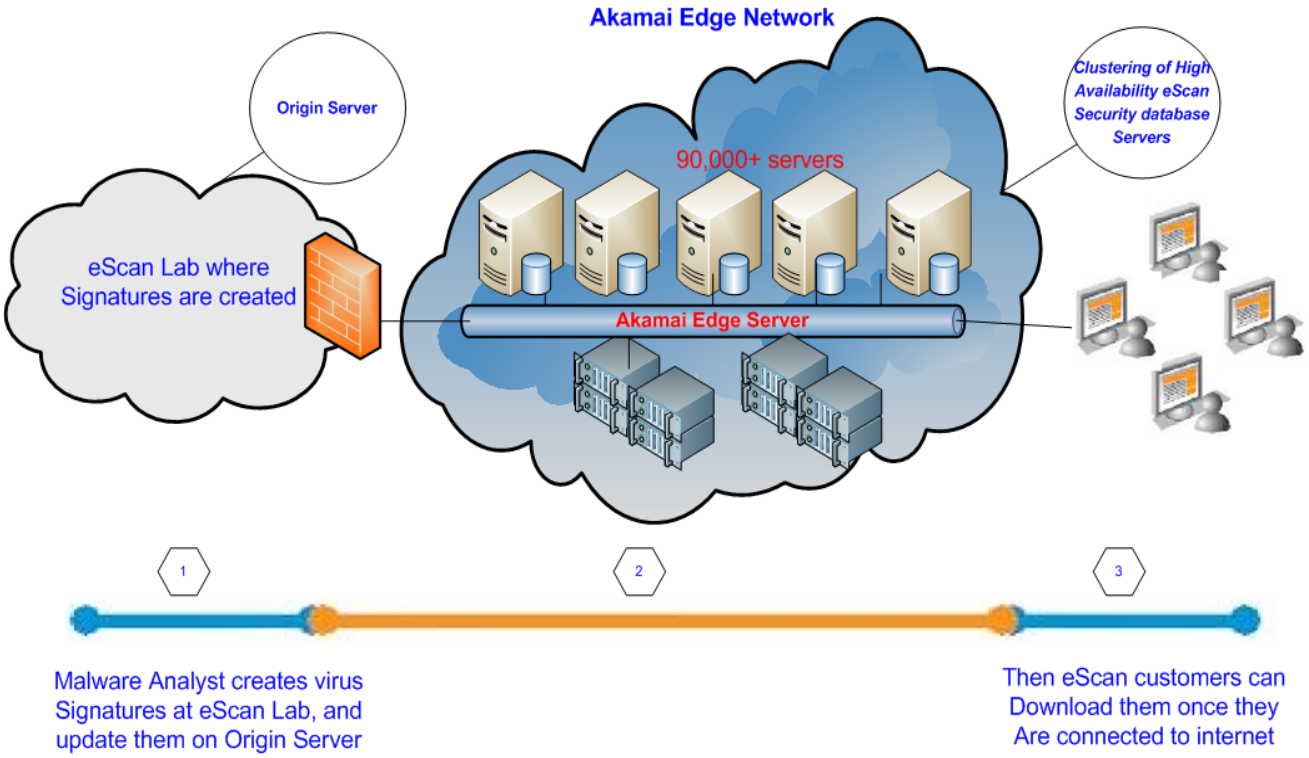
امروزه، به طور متوسط روزانه بیش از ۱۰۰ نوع بدافزار یافت می‌شود و برای تولیدکنندگان آنتی‌ویروس، وظیفه بسیار مشکلی است تا برای هر ویروس، الگوهای شناسایی متناظر را انتشار نمایند، اما این مقوله به منظور پیشگیری از تهدیدهای روزافزون الزامی می‌باشد.

زیرساخت مناسب نقش مهمی در توزیع به‌روزرسانی‌ها به تمام مشتریان ایفاء می‌نماید. دلیل این امر، تعداد فراوان مشتریان استفاده کننده از موتور آنتی‌ویروس eScan می‌باشد، این فراوانی بر اساس گستردگی eScan در سراسر جهان می‌باشد. به منظور خدمات‌رسانی مناسب به تمام مشتریان در سرتاسر جهان، بیش از ۹۰,۰۰۰ سرور به‌روزرسانی برای تمام محصولات eScan در نظر گرفته شده که این مهم در هنگام توزیع الگوهای شناسایی بدافزار (امضاهای ویروس) با موضوعاتی چون بررسی سرعت دانلود الگوهای شناسایی بدافزار (امضاهای ویروس) و قابلیت دسترس‌پذیری به سرورهای بیش‌تر توسط طیف وسیعی از کاربران پیاده‌سازی می‌گردد.

ساز و کار به‌روزرسانی این ۹۰,۰۰۰ سرور در سراسر دنیا بسیار نیرومند است. Akamai نیز نقش حیاتی در این فرآیند دارد. لابراتوار eScan، فرآیند به‌روزرسانی الگوهای شناسایی بدافزار (امضاهای ویروس) را به سرور لبه Akamai اجرا نموده و سپس این سرور در طی زمان کم‌تر از چند دقیقه عملیات همگام‌سازی به‌روزرسانی‌ها را به تمام این ۹۰,۰۰۰ سرور در سراسر دنیا به انجام می‌رساند.

شکل صفحه‌ی بعد نحوه‌ی توزیع الگوهای شناسایی بدافزار (امضاهای ویروس) را با توضیح مرتبط، نمایش می‌دهد:

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) - ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir



شکل فوق بیانگر نحوه‌ی توزیع به‌روزرسانی‌ها و همگام‌سازی آن‌ها بین سرورهای مختلف است. eScan بیش از ۹۰,۰۰۰ سرور را به منظور توزیع الگوهای شناسایی بدافزار (امضاهای ویروس) به کاربران استقرار داده است. در ادامه، توضیحات گام به گام شکل فوق تشریح شده است:

۱. کارشناسان و تحلیلگران بدافزار eScan، در فرآیندی که پیش‌تر بیان شد، الگوهای شناسایی بدافزار (امضاهای ویروس) را ایجاد می‌نمایند.

۲. لابراتوار eScan الگوهای شناسایی بدافزار (امضاهای ویروس) تولید شده را بر روی سرور اصلی eScan بارگذاری می‌نماید.

شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) – ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir

۳. سرور اصلی eScan نیز، الگوهای شناسایی بدافزار (امضاهای ویروس) را با استفاده از پروتکل FTP و هر ۲ ساعت یک‌بار بر روی سرور لبه Akamai بارگذاری می‌نماید.

۴. الگوهای شناسایی بدافزار (امضاهای ویروس) به طور خودکار بر روی شبکه لبه Akamai، کپی یا mirror می‌گردند.

۵. کلاینت‌های eScan الگوهای شناسایی بدافزار (امضاهای ویروس) مذکور را از طریق شبکه Akamai دانلود می‌نمایند.

نحوه‌ی انتشار الگوهای شناسایی بدافزار (امضاهای ویروس) توسط eScan به شرحی که گذشت در مستند، بیان شد. هر بار که الگوهای شناسایی بدافزار (امضاهای ویروس) برای دانلود در دسترس باشند، محصولات eScan به طور خودکار هر ۲ ساعت یک‌بار، درخواست پرس و جو به سرورهای به‌روزرسانی eScan ارسال نموده تا وضعیت دسترس‌پذیری به الگوهای شناسایی بدافزار (امضاهای ویروس) جدید، بررسی شود. در این فرآیند شرایط زیر بررسی و به شرح زیر اجرا می‌شود:

۱. درخواست پرس و جو به سرورهای به‌روزرسانی eScan توسط محصولات eScan ارسال شده تا وضعیت دسترس‌پذیری به الگوهای شناسایی بدافزار (امضاهای ویروس) جدید بررسی شود.

۲. اگر الگوهای شناسایی بدافزار (امضاهای ویروس) جدیدی یافت شد، eScan فرآیند دانلود خودکار الگوهای شناسایی بدافزار (امضاهای ویروس) جدید را اجرا نموده و پایگاه داده ویروس، به‌روزرسانی می‌شود.

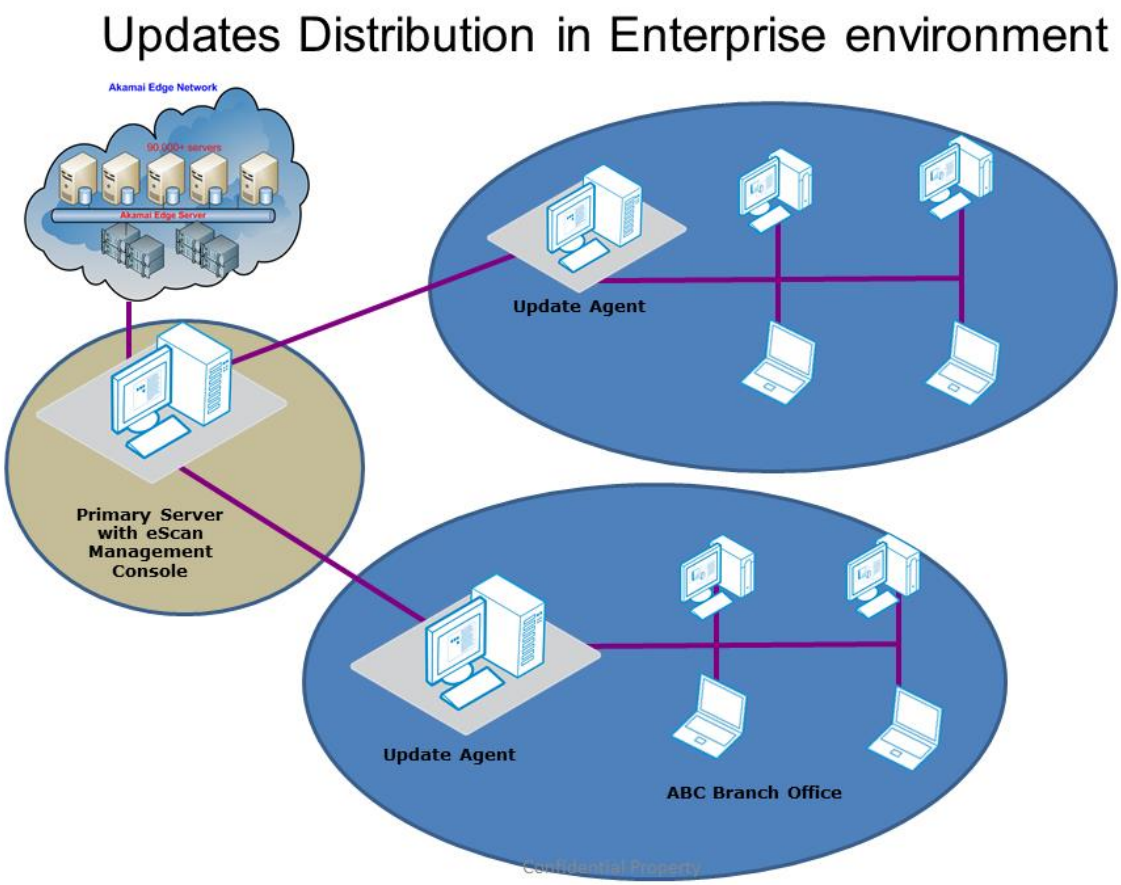
۳. اگر الگوهای شناسایی بدافزار (امضاهای ویروس) جدیدی موجود نبود، پس از ۲ ساعت، فرآیند گام ۲، تکرار می‌گردد.

۴. اگر در زمان درخواست پرس و جو، اتصال به اینترنت موجود نباشد یا به هر نحوی مشکلی در این زمینه موجود باشد، هر ۳ دقیقه یک‌بار، این فرآیند تکرار می‌شود تا زمانی‌که درخواست پرس و جو با موفقیت ارسال شود.

در محصولات تحت شبکه و سازمانی، تمام مراحل فوق انجام می‌شود با این تفاوت که کلاینت‌های eScan به‌روزرسانی‌های موجود را از طریق سرور eScan دانلود می‌نمایند نه اینترنت؛ و سرور

eScan نیز، از اینترنت به‌روزرسانی‌های موجود را دریافت می‌نماید و تمام ۴ گام فوق، عملیاتی می‌شود. لازم به ذکر است که در محیطها و بسترهای تحت شبکه و سازمانی، ممکن است کلاینت eScan در شبکه محلی قرار نداشته باشد و در این‌صورت کلاینت باید به طور مستقیم با اتصال به اینترنت الگوهای شناسایی بدافزار (امضاهای ویروس) را دانلود نماید و این فرآیند پس از ۶ ساعت انجام خواهد شد، به این‌گونه که این زمان، صرف تشخیص عدم حضور کلاینت در شبکه محلی که سرور eScan در آن استقرار یافته، می‌گردد.

شکل زیر بیانگر نحوه‌ی دانلود به‌روزرسانی‌های شعبه‌های مختلف از سرور تحت شبکه eScan و عوامل (نمایندگان) به‌روزرسانی است: (توزیع به‌روزرسانی‌ها در محیطهای سازمانی)



شماره تماس: ۴۴۹۵۵۵۶۷ (۰۲۱) – ۳۶۲۸۱۱۱۲ (۰۳۵)
ایمیل: info@kaipod.ir