به نام خداوند یکتا

مستند

قابلیت ضدهرزنامه

آنتی‌ویروس eScan

(Anti-Spam)

تاریخ انتشار: خردادماه ۱۳۹۵

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

فهـرسـت

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

۱- مقدمه

هدف از این مستند، بررسی چالش‌ها و مشکلات مرتبط با هرزنامه‌ها (Spam E-mails)، بیان فناوری‌های موجود به منظور مقابله با هرزنامه‌ها و توضیح نحوه‌ی عملکرد فناوری منحصربه‌فرد eScan در این مقوله‌ی مهم می‌باشد.

هرزنامه چیست؟ رایانامه‌های تبلیغاتی، مزاحم و ناخواسته‌ی عمدتاً با اهداف تجاری، به طور معمول به عنوان هرزنامه معرفی می‌شوند که به سرعت در حال رشد و گسترش به سامانه‌های رایانه‌ای رومیزی در منازل، دفاتر کار و سازمان‌ها است. تأثیر عمده‌ی هرزنامه‌ها بر روی ISPهایی است که باید با افزایش میزان ترافیک کارگزار رایانامه بر مشکلات ایجاد شده بر پهنای باند توسط هرزنامه‌ها فائق آیند. کسب و کارها نیز از حمله‌های مبتنی بر هرزنامه که زیرساخت‌ها و بهره‌وری آن‌ها را تحت تأثیر قرار می‌دهند، رنج می‌برند. هرزنامه، استفاده از سامانه‌های پیام‌رسان الکترونیکی برای ارسال انبوه پیام ناخواسته، به‌ویژه تبلیغاتی، به‌صورت غیرمشخص است؛ در اکثر موارد منظور از هرزنامه، قالب رایانامه هرزنامه می‌باشد.

فرآیند ایجاد و انتشار هرزنامه، از لحاظ اقتصادی قابلیت بقا دارد، زیرا تبلیغات کننده‌ها هیچ هزینه‌ی عملیاتی فراتر از مدیریت لیست‌های رایانامه‌ای ندارند. از آن‌جا که موانع جلوگیری از ورود هرزنامه‌ها بسیار ضعیف است، هرزنامه‌نگارهای متعددی وجود دارند و حجم رایانامه‌های ناخواسته‌ای که دریافت می‌شود، بسیار فراوان شده است. در سال ۲۰۱۲، این تعداد برای پیام‌های هرزنامه حدود هفت تریلیون برآورد شده است. هزینه‌ها، مانند کاهش بهره‌وری و جعل توسط رسانه‌های عمومی و نیز ISPها بوجود می‌آیند، که این موضوع افزایش ظرفیت افزون‌تر برای مقابله با هرزنامه‌ها را الزامی نموده است. لازم به ذکر است؛ فرد یا برنامه‌ای که هرزنامه‌ی الکترونیکی ایجاد می‌نماید، هرزنامه‌نگار نامیده می‌شود. (منبع: ویکی‌پدیا)

۲- چگونه برای توقف هرزنامه از فناوری ضدهرزنامه eScan استفاده کنیم؟

تکنیک‌های مختلفی برای مقابله با هرزنامه‌ها وجود دارد؛ هیچ یک از آن‌ها به طور کامل نمی‌توانند بدون مسدودسازی هر رایانامه‌ی معمولی، از ورود هرزنامه جلوگیری کنند، در واقع، در گام اول

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

فرآیند تشخیص نادر ست (False Positive) می‌تواند اتفاق بیفتد. با این حال، با کاربرد ترکیبی از تکنیک‌های هرزنامه، می توان ورود هرزنامه را در پایین‌ترین ســطح ممکن قرار داد و از هر گونه تشخیص نادرست نیز جلوگیری نمود.

روش‌های متداول مورد استفاده برای شناسایی و مسدودسازی هرزنامه‌ها، عبارتند از:

- NILP (الگوی فراگیری هوشمند)
- RBL (لیست‌های رد بلادرنگ)
- اعتبارسنجی IP (IP Reputatin)
- جستجوی Reverse DNS (Reverse DNS Lookup)
- فرستنده جعلی (Spoofed Sender)
- فریم‌ورک خط‌مشی فرستنده (Sender Policy Framework)
- بررسی سرآیند (Header Check)
- پایگاه داده هرزنامه (Spam Database)
- کاراکترهای روسی یا چینی
- SURBL
- بررسی محتوا (Content Checking)
- تجزیه و تحلیل تصویر (Image Analysis)

eScan ترکیبی از فناوری‌های مذکور را به منظور پیشگیری از ورود هرزنامه استفاده می‌نماید. اغلب روش‌ها در بخشی از محصولات eScan موجود می‌باشند. در ادامه این روش‌ها بیان خواهد شد:

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

- **NILP (الگوی فراگیری هوشمند)**

فناوری نوآورانه‌ای از MicroWorld که مبتنی بر اصول هوش مصنوعی فعالیت نموده؛ ساز و کاری تطبیقی در کنترل هرزنامه و حمله‌های صیادی (فیشینگ) ایجاد می‌نماید. این فناوری هر رایانامه را بر اساس الگوهای رفتاری کاربر، تجزیه و تحلیل نموده و سپس بر اساس نتایج حاصل، تصمیم مورد نظر درباره‌ی آن را اتخاذ می‌نماید. NILP دارای ساز و کاری خودفراگیر و مجزا از کارگزار MicroWorld می‌باشد.

- **NILP چگونه کار می‌کند؟**

بر اساس روش فیلتر سازی (پالایش) Bayesian مبتنی بر اصول هوش مصنوعی کار می‌کند. این روش دارای قابلیت‌های خودفراگیر بوده و از ساز و کاری تطبیقی به منظور طبقه‌بندی رایانامه‌ها بر اساس الگوهای رفتاری کاربر، استفاده می‌نماید. NILP خود را با استفاده از نتایج جستجوی متداول از کارگزارهای MicroWorld به‌روز می‌نماید. هرگاه که رایانامه‌ی جدیدی دریافت می‌شود، NILP آن را بر اساس فراگیری تجمعی، تجزیه و تحلیل نموده و به دو دسته‌ی هرزنامه یا رایانامه‌ی عادی، تقسیم‌بندی می‌نماید.

NILP هم‌چنین پایگاه داده‌ای از الگوهای ساختاری یا DNA میلیون‌ها هرزنامه را نگهداری می‌نماید که به طور مداوم، به‌روزرسانی می‌شوند. این روش با استفاده از الگوهای ساختاری یا DNA موجود در پایگاه داده‌ی به‌روزرسانی شده، الگوریتم فراگیری خود را فراخوانی نموده و سپس تعیین می‌نماید که رایانامه‌ی دریافتی، هرزنامه است یا خیر. به این طریق، فناوری NILP، از کاربر به منظور جلوگیری از دریافت هرزنامه و رایانامه‌های فیشینگ و کلاهبرداری محافظت می‌نماید.

- **RBL (لیست‌های رد بلادرنگ)**

در این روش، آدرس‌های IP ورودی بررسی شده تا بر اساس مطابقت با لیست‌های عدم پذیرش یا رد، تعیین گردد که کارگزار فرستنده‌ی رایانامه در لیست قرار دارد یا خیر؛ و در عمل با این استراتژی دریافت هرزنامه متوقف گردد. به طور معمول هر کارگزار رایانامه‌ی امن

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

باید از ارسال رایانامه توسط فرستنده بیرونی به هر عاملی خارج از حوزه‌ی خود جلوگیری نماید. این موضوع، تضمین می‌نماید که هرزنامه‌نگارها نتوانند این فرآیند را جعل نمایند و ارسال هرزنامه را از یک کارگزار، به عنوان رایانامه‌ی قانونی جلوه دهند. متأسفانه برخی مدیران سیستم، به هر دلیلی، به علت ضعف در پیکربندی کارگزارهای رایانامه‌ی خود از مسدودسازی چنین ارسال‌هایی ناتوان می‌باشند. eScan از مجموعه‌ی پیش‌فرض دو سرویس رایگان و قابل اعتماد RBL استفاده می‌نماید که توانایی پیکربندی جهت استفاده از چندین لیست رد بلادرنگ در یک زمان را برای اطمینان و دقت بیش‌تر فراهم می‌نماید.

- **اعتبارسنجی IP**

این روش بسیار ساده است. تمام رایانامه‌ها باید از یک آدرس IP مشخص ارسال شده باشند. اعتبارسنجی IP به این دلیل استفاده می‌شود که بیان نماید کدام آدرس IP، مسئول ارسال هرزنامه یا رایانامه‌های انبوه ناخواسته است و در بهترین حالت مؤثر از دریافت ۸۰% از هرزنامه‌ها جلوگیری می‌نماید. آدرس IP به طور گسترده‌ای جهت تعیین منبع کلی هرزنامه استفاده می‌شود. با این روش می‌توان در برخی شبکه‌ها بر اساس آدرس‌های IP که توسط هرزنامه‌نگارها استفاده می‌شوند، پیام‌هایی که با عنوان هرزنامه یا قرنطینه شده برچسب خورده‌اند را رد و یا مسدود نمود. eScan پایگاه داده‌ای مبتنی بر رایانامه‌های دریافتی جهت حفظ پایش سیستم‌های مورد بررسی ایجاد نموده است. eScan بر اساس اعتبارسنجی آدرس‌های IP، آن‌ها را رتبه‌بندی می‌نماید. این فرآیند در یک پایگاه داده ذخیره می‌شود و این پایگاه داده، هر زمان داده‌ای اضافه یا حذف شود، به‌روزرسانی می‌گردد.

- **جستجوی Reverse DNS**

این روش، خیلی مناسب نمی‌باشد، زیرا بسیار زمان‌بر است. کارگزار دریافتی برای آدرس IP اتصالات ورودی، جستجوی Reverse DNS را انجام می‌دهد تا اعتبار نام میزبان ثبت شده‌ی مرتبط با آن را بررسی نماید. این فرآیند یعنی جستجوی Reverse DNS زمان زیادی نیاز دارد. eScan هم‌چنین از جستجوی HELO استفاده می‌نماید که یک روش ممتاز می‌باشد، به این صورت که کارگزار دریافت کننده، نام میزبان کارگزار رایانامه‌ی ارسالی را با استفاده از دستور

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

SMTP HELO بدست می‌آورد. این فرآیند یک پرس و جوی ساده را انجام داده و مشخص می‌نماید که آیا آدرس IP فراخوانی شده، همان آدرس IP اتصال ورودی است یا خیر؟.

- **فرستنده‌ی جعلی**

جعل آدرس رایانامه یکی از روش‌های شایع در سازمان‌ها به منظور ارسال پیام‌های رایانامه‌ای از منابع بیرونی با ظاهرسازی به عنوان آدرس‌های درونی و شناخته شده می‌باشد. نمونه‌های متعددی از جعل آدرس رایانامه وجود دارد، به عنوان مثال ارسال رایانامه به abc@escanav.com با جعل به عنوان xyz@escanav.com.

eScan راهکار جامع ضدجعل و مسدودسازی رایانامه‌های فیشینگ و کلاهبرداری را برای شبکه‌های درون سازمانی ارائه می‌نماید.

- **فریم‌ورک خطمشی فرستنده (SPF)**

این روش، یک سیستم اعتبارسنجی است که به منظور جلوگیری از دریافت هرزنامه با تشخیص جعل یا یک آسیب‌پذیری با ممیزی نمودن آدرس‌های IP فرستنده، طراحی شده است. فریم‌ورک خطمشی فرستنده (SPF) به مدیران شبکه این امکان را می‌دهد تا مشخص نمایند که کدام میزبان اجازه‌ی ارسال رایانامه را از حوزه‌ی داده شده از طریق ایجاد یک رکورد SPF خاص در سیستم نام‌گذاری دامنه (DNS) دارد. مبادله کننده‌ی رایانامه یا Mail Exchanger با استفاده از DNS بررسی می‌کند که رایانامه از میزبانی که مورد تأیید دامنه‌های مدیر و اصلی است، ارسال شده است یا خیر؟.

- **بررسی سرآیند**

بازنگری و ممیزی سرآیند، فرآیندی مناسب به منظور بررسی سرآیندهای رایانامه‌های مبتنی بر پروتکل SMTP است تا میزان تطابق آن‌ها با استانداردهایی که تضمین می‌نمایند آن‌ها توسط هرزنامه‌نگارها جعل نشده‌اند، مشخص شود. هم‌چنین برخی برنامه‌های ارسال هرزنامه، مواردی از اطلاعات قابل شناسایی مشخص را در سرآیند SMTP رایانامه و سایر داده‌ها درج می‌نمایند.

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

- **پایگاه داده هرزنامه**

فناوری پایگاه داده هرزنامه، عبارات کلیدی را از رایانامه‌های دریافتی استخراج نموده و آن‌ها را با هرزنامه‌های موجود در پایگاه داده، مقایسه می‌نماید. بر اساس استنباط آماری در این مقایسه، اگر احتمال وجود عبارات هرزنامه‌ای زیاد باشد، رایانامه به عنوان هرزنامه نشان‌گذاری می‌شود. این راهکار، یک فناوری قدرتمند خواهد بود اگر به طور مناسب پیاده‌سازی گردد، زیرا توانایی مسدودسازی بلادرنگ هرزنامه در این فناوری وجود دارد.

- **تغییر و دستکاری در متن**

اغلب پیام های هرز نامه، با استفاده از تحلیل متنی محتوا، روش هایی را به منظور فریب ابزارهای ضدهرزنامه به کار می‌برند. تغییر و دستکاری در متن و جایگزینی آن با کاراکترهای مشابه از لحاظ شکل ظاهری، جداسازی کاراکترها جهت افزایش سختی تحلیل آن به عنوان یک کلمه‌ی کامل، کاربرد نمادهای مشابه یا اعداد و حروف در نمایش بخشی از کلمات و عبارات یا تمام آن‌ها، از موارد فریفتن ابزارهای ضدهرزنامه می‌باشد. برخی از این موارد، عبارتند از:

- نمایش صفر به‌جای حروف کوچک و بزرگ O، به عنوان مثال W0RD به‌جای WORD
- استفاده از نماد \/\/ به‌جای حروف کوچک و بزرگ W

eScan توانایی کامل شناسایی و پیشگیری از تمام انواع هرزنامه‌های فوق را دارا می‌باشد.

- **کاراکترهای چینی یا روسی**

اگر کاراکترهای چینی یا روسی در رایانامه موجود باشند، eScan قابلیت شناسایی کاراکترهای مذکور را دارد و رایانامه را به عنوان هرزنامه شناسایی می‌کند.

- **بررسی محتوا**

یک روش قدیمی که با بررسی محتوا و یافتن کلیدواژه در متن رایانامه، فرآیند مسدود سازی آن انجام می‌گیرد. این روش در برخی موارد باید به صورت دستی انجام شود.

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

- **SURBL**

یک نوع روش شناسایی هرزنامه می‌باشد که به طور خاص، لیست مسدودسازی بلادرنگ مشخصه‌های وب‌سایت‌های حاوی تبلیغات و هرزنامه را شامل می‌شوند. این عبارت مخفف Spam Uniform Resource Identifier (URI) Real-time Block List می‌باشد. SURBL به منظور جستجوی بدنه‌ی پیام‌های رایانامه‌ی ورودی برای لینک‌های حاوی تبلیغات و هرزنامه جهت ارزیابی این که رایانامه، عادی یا تبلیغاتی (هرزنامه) است، استفاده می‌شود. به عنوان مثال اگر آدرس وب‌سایت Http://www.test.com در لیست رد قراد داشته باشد، آن‌گاه پیام رایانامه حاوی بدنه‌ی این URL، به عنوان هرزنامه شناسایی می‌شود. eScan مشخصه‌های وب سایت‌های حاوی تبلیغات و هرزنامه را استخراج نموده و سپس بررسی می‌نماید که آیا در لیست قرار دارند یا خیر؛ بر اساس نتایج این بررسی، رایانامه به عنوان هرزنامه برچسب‌گذاری می‌شود.

- **تجزیه و تحلیل تصویر**

طیف عمده‌ای از هرزنامه‌ها شامل محتوای تصاویر غیراخلاقی می‌باشند. قابلیت ضدهرزنامه پیشرفته‌ی eScan توانایی شناسایی هرزنامه با تصاویر و لینک‌های مرتبط با تصاویر را دارا می‌باشد. این قابلیت پیشرفته با دسترسی خزش خودکار وب و با استفاده از الگوریتم‌های تطبیق الگو، محتواهای نامناسب تصویری و هرزنامه را شناسایی می‌نماید. این قابلیت بسیار هوشمند بوده و توانایی تمایز بین محتوا و تصاویر پزشکی با سایر موارد نامناسب را دارا می‌باشد. پس از تجزیه و تحلیل تصاویر در خزش خودکار وب، در صورت تشخیص محتوای تصویر به عنوان غیراخلاقی و هرزنامه، سایت مورد نظر نمایه شده و در پایگاه داده URL اضافه می‌گردد.

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