Regin یک ابزار جاسوسی پیشرفته

تهیه‌کننده: الهه دائی

Regin یک نرم‌افزار بسیار پیچیده با طیف گسترده‌ای از قابلیت‌ها است که می‌توان آن را برای اهداف مختلف سفارشی‌سازی نمود.

رجین، یک ابزار جمع‌آوری اطلاعات چند منظوره است که سال‌ها در حال فعالیت است. اولین بار سیمانتک و به فاصله کمتر از یک روز کسپراسکای گزارشات تحلیلی از این بدافزار را در زمستان 2014 منتشر کردند. تاکنون نسخه‌های متعددی از رجین مشاهده شده است. که افراد، دانشگاهیان، موسسات و شرکت‌های مختلفی را هدف قرار داده است.

رجین قابلیت‌های استاندارد گسترده‌ای به ویژه در زمینه شنود و سرقت اطلاعات دارد. برخی پیلودهای سفارشی رجین اشاره به سطح بالایی از دانش تخصصی در حوزه‌های مختلف همچون زیرساخت‌های مخابراتی دارد.

رجین تا حد زیادی برای هر هدف قابل سفارشی‌سازی است. این ویروس برای سرقت پسورد، نظارت بر ترافیک شبکه و جمع‌آوری اطلاعات از فرایندها و حافظه، سازماندهی شده است. همچنین قادر به اسکن فایل‌های پاک شده[1] در کامپیوتر قربانی و بازیابی آن‌ها است. تحقیقات نشان می‌دهد بسیاری از ماژول‌های آن با اهداف خاص طراحی شده‌اند. برای مثال، یک ماژول برای نظارت بر ترافیک شبکه از طریق سرویس اطلاعات اینترنت مایکروسافت (IIS) بر روی سرورهای وب طراحی شده است. ماژول دیگری برای جمع‌آوری ترافیک مدیریت کنترل کننده‌های ایستگاه‌های پایه تلفن همراه و یا ماژول دیگری به‌طور خاص برای جداسازی ایمیل‌ها از اطلاعات مبادله شده، ایجاد شده است.

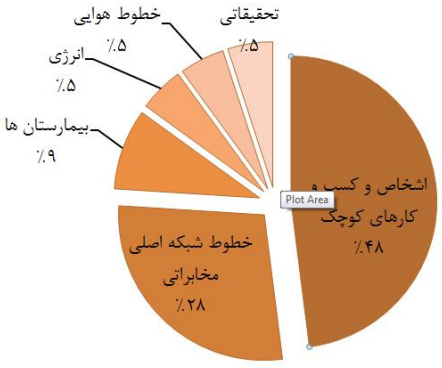
رجین با طول‌های مختلف برای پنهان‌سازی سرقت اطلاعات به‌کار می‌رود. در برخی موارد سیمانتک قادر به بازیابی فایل‌های حاوی اطلاعات به سرقت رفته نبود و تنها نمونه‌های تهدید را توانسته بازیابی کند.

اطلاعات منتشر شده توسط شرکت امنیتی سیمانتک تنها شامل اطلاعات در مورد دو نسخه از رجین است. نسخه 1 که به نظر می‌رسد بین سال‌های 2008 تا 2011 به‌کار رفته است. نسخه 2 که از سال 2013 آغاز به کار کرده است. چنین به نظر می‌رسد که نسخه 1 در سال 2011 به صورت ناگهانی از چرخه خارج شده است.

شواهد حاکی از آن است که به احتمال زیاد رجین بیش از دو نسخه دارد که ممکن است نسخه‌هایی قبل از نسخه 1 و یا نسخه-هایی بین نسخه 1 و 2 وجود داشته باشد. از طرفی آنتی‌ویروس کسپراسکای نیز زمان ظهور این ویروس را نامشخص اعلام کرده و برخی مهرهای زمانی[2] مربوط به این ویروس را متعلق به سال 2003 می‌داند.

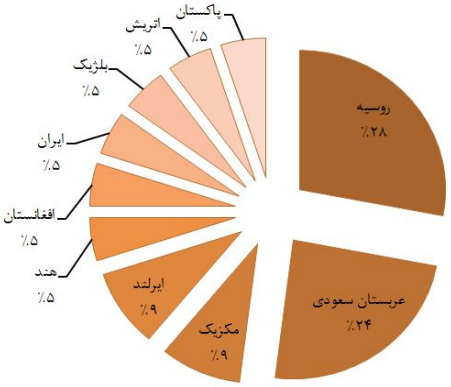
مشخصات قربانیان رجین

اپراتورهای رجین تنها به بخش خاصی از صنعت تمرکز ندارند. آلودگی به رجین در سازمان‌های متعددی مشاهده شده که شامل شرکت‌های خصوصی، بخش‌های دولتی و موسسات تحقیقاتی است. آلودگی به این ویروس از نظر جغرافیایی نیز دارای پراکندگی است و به صورت عمده در 10 ناحیه مختلف شناسایی شده است.



شکل1. آلودگی به رجین بر اساس حوزه‌های مختلف

1 - Delete
2- Time Stamp



شکل **2**. آلودگی به رجین بر اساس کشور

بردار آلودگی در قربانی‌های مختلف، متفاوت است. قربانی‌ها ممکن است با مشاهده نسخه جعلی وبسایت‌های شناخته شده مانند LinkedIn فریب بخورند یا تهدید ممکن است از طریق مرورگر وب یا با استفاده از برنامه‌های مخرب، بر روی سیستم مورد نظر نصب شود. گزارشات نشان می‌دهد در مواردی رجین از طریق یاهو مسنجر سیستم را آلوده ساخته است.

بررسی ماهیت رجین و پیلودهای سفارشی‌سازی آن، نشان می‌دهد که برخی پیلودها به احتمال زیاد به منظور فراهم آوردن امکان ارتقا قابلیت‌های رجین به‌کار رفته‌اند.

رجین ممکن است هر یک از اقدامات زیر را انجام دهد:

- شنود ترافیک شبکه
- فیلتر اطلاعات از طریق کانال‌های مختلف (TCP، UDP، ICMP و HTTP)
- جمع‌آوری اطلاعات کامپیوتر
- سرقت پسوردها
- جمع‌آوری اطلاعات حافظه و فرایندها
- راهبری از طریق سیستم فایل
- انجام عملیاتی چون بازیابی فایل‌هایی که حذف شده‌اند
- دستکاری رابط کاربر (UI) همچون هدایت از راه دور حرکات و کلیک‌های موس و ضبط تصاویر صفحه نمایش
- شنود سرورهای وب و سرقت لاگ‌ها
- شنود ترافیک شبکه مدیریت GSM BSC

نتیجه‌گیری

رجین یک تهدید بسیار پیچیده است که برای جمع‌آوری هوشمندانه اطلاعات در مقیاس بزرگ به‌کار می‌رود. توسعه و بهره‌برداری از این تهدید نیاز به سرمایه‌گذاری زمان و منابع قابل توجهی داشته است. تهدیداتی از این دست بسیار نادر هستند و تنها با خانواده نرم‌افزارهای مخرب Stuxnet/Duqu قابل مقایسه است. کشف رجین، نشان می‌دهد سرمایه‌گذاری‌های قابل توجهی برای توسعه ابزارهایی با هدف جمع‌آوری هوشمندانه اطلاعات در دست انجام است. بسیاری از مولفه‌های رجین هنوز کشف نشده است و ممکن است قابلیت‌ها و نسخه‌های بیشتری از آن وجود داشته باشد.

توصیه‌ها

توصیه می‌شود مدیران و کاربران موارد امنیتی پایه زیر را رعایت کنند:

- از نرم‌افزارهای رایگان و کرک شده تا حد امکان استفاده نشود. بدون تردید تعدادی از نرم‌افزارهای کرک شده و رایگان، آلوده به بدافزارهای مخرب و جاسوسی هستند.
- با استفاده از فایروال تمام ارتباطات از اینترنت به سرویس‌هایی که نباید در دسترس عموم باشد مسدود شود. به صورت پیش‌فرض، باید تمام ترافیک ورودی مسدود شود به جز سرویس‌هایی که لازم است از بیرون به آن‌ها دسترسی وجود داشته باشد.

- به اجرا در آوردن سیاست‌های کلمه عبور. کلمات عبور پیچیده، امکان شکستن فایل‌های کلمات عبور را دشوار می‌سازد. این کار به کاهش خسارات وارد شده به سیستم کمک می‌کند.
- اطمینان حاصل کنید که کاربران و برنامه‌های کامپیوتری حداقل دسترسی مورد نیاز برای انجام وظایف خود داشته باشند و تنها به برنامه‌های مجاز، سطح دسترسی مدیریت[3] داده شود.
- برای جلوگیری از اجرای اتوماتیک فایل‌های اجرایی بر روی شبکه و درایوهای قابل جابجایی، AutoPlay را غیرفعال کنید. همچنین این نوع درایوها را زمانی که مورد نیاز نیستند جدا کنید و در صورت عدم نیاز به دسترسی نوشتن، دسترسی فقط خواندنی[4] را فعال کنید.
- در صورت عدم نیاز به اشتراک فایل‌ها، به اشتراک‌گذاری آن‌ها را غیرفعال کنید. در صورت نیاز به اشتراک فایل‌ها، از ACL و رمز عبور برای محدود ساختن دسترسی‌ها استفاده کنید. دسترسی ناشناس به فولدرهای به اشتراک گذاشته شده را غیرفعال کنید و تنها به کاربران با رمز عبورهای قوی اجازه دسترسی به این فولدرها داده شود.
- سرویس‌های غیرضروری را غیرفعال و حذف کنید. بسیاری از سیستم عامل‌ها، به صورت پیش فرض بسیاری از سرویس‌ها که ضروری نیستند را نصب می‌کنند. این سرویس‌ها راه‌هایی برای حمله ایجاد می‌کنند که در صورت حذف این سرویس‌ها، تهدیدات حملات نیز کاهش خواهد یافت.
- اگر تهدیدی از یک یا چند سرویس شبکه بهره‌برداری می‌کند، آن سرویس را غیرفعال یا دسترسی به آن را بلاک کنید تا زمانی که تمهیدات امنیتی اندیشیده شود.
- همیشه تمهیدات امنیتی خود را به روز نگه دارید، به خصوص برای کامپیوترهایی که میزبان سرویس‌های عمومی هستند و از طریق فایروال قابل دسترسی هستند همچون سرویس‌های HTTP، FTP، Mail و DNS
- سرور ایمیل خود را طوری پیکربندی کنید که ایمیل‌هایی که حاوی فایل‌های پیوستی که معمولا برای انتشار ویروس به‌کار می‌روند، هستند همچون فایل‌های vbs، bat، exe، pif و scr را بلاک نموده یا حذف کند.
- کامپیوترهای به خطر افتاده را برای جلوگیری از گسترش بیشتر تهدید، سریعا ایزوله کنید. آن‌ها را تحلیل جرم‌شناسی[5] کنید و با استفاده از رسانه‌های مورد اعتماد بازیابی کنید.
- کارمندان نباید فایل‌های پیوست را باز کنند مگر اینکه انتظار آن را داشته باشند. همچنین نرم‌افزارهایی که از طریق اینترنت دانلود می‌کنند را نباید اجرا کنند مگر اینکه اسکن شده و ویروسی نباشد. در صورتی که آسیب‌پذیری‌های مرورگر خاص (از طریق patchهای امنیتی) برطرف نشده باشد مشاهده یک سایت وب مخرب می‌تواند به سادگی منجر به آلودگی شود.
- در صورت عدم نیاز به بلوتوث تلفن همراه، آن را خاموش کنید. در صورت نیاز به استفاده از آن، اطمینان حاصل نمایید که قابلیت مشاهده[6] دستگاه غیرفعال است و نمی‌تواند از طریق سایر دستگاه‌های بلوتوث اسکن شود. همچنین برنامه‌ها را از منابع ناشناخته نپذیرید.

منابع

[1]. Symantec Security Response, Regin: Top-tier espionage tool enables stealthy surveillance
[2]. Kaspersky Lab Report, THE REGIN PLATFORMNATION-STATE OWNAGE OF GSM NETWORKS

3 - Administration
4 - Read-only
5 - Forensic
6 -Visibility