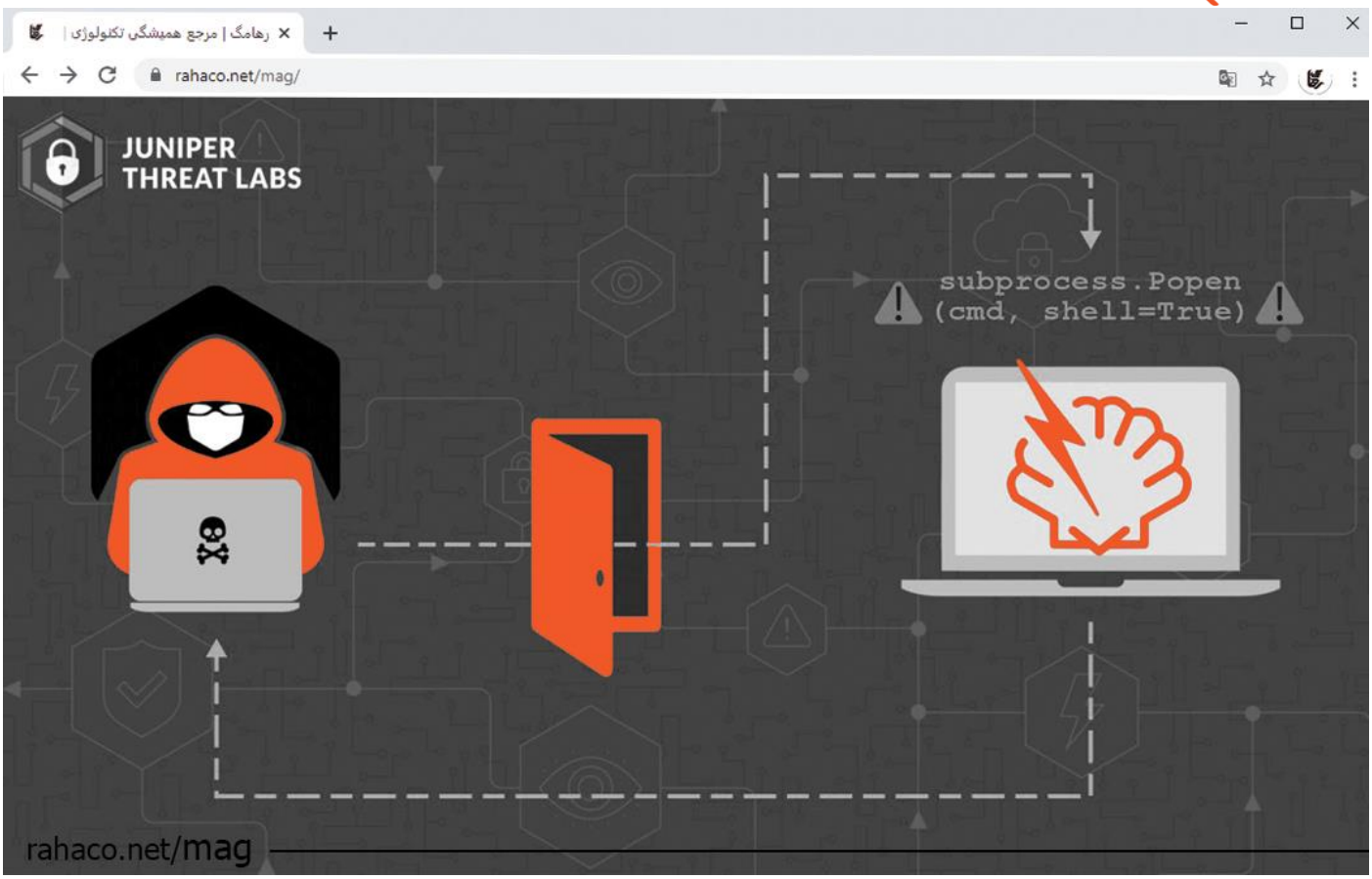
جدیدترین حمله با اسکریپت پایتون به سرورهای VMware ESXi

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

در دنیای امروز بر کسی پوشیده نیست که مجازی سازی می‌تواند زیرساخت فناوری اطلاعات را بهبود بخشد و کارایی را افزایش دهد. با این حال، فرآیند مجازی سازی متغیرهای زیادی دارد که باید قبل از ورود به این مسیر در نظر گرفته شود. در گذشته به دلیل تعداد محدود محصولات و راهکارهای موجود در بازار، استفاده از راهکار مجازی سازی نسبتا آسان بود. امروزه ارائه دهندگان مجازی سازی با محصولات و امکانات بی شماری در دسترس هستند و مدیران IT باید راهکاری را انتخاب کنند که به بهترین وجه با نیازهای تجاری آن‌ها مطابقت داشته باشد.

یکی از پلتفرم‌های محبوب در حوزه مجازی سازی VMware ESXi است که معمولا برای میزبانی سرورها مورد استفاده قرار می‌گیرد. این پلتفرم به طور موثر از منابع CPU و حافظه موجود در دستگاه استفاده می‌کند. اخیرا محققان Juniper Networks یک حمله مخرب و غیرمجاز را در سرورهای VMware ESXi پیدا کردند اما هنوز متوجه نشدند که چگونه این حمله رخ داده است. در این مقاله با ویژگی‌های VMware ESXi بیشتر آشنا می‌شوید و در مورد آخرین حمله باج افزار مبتنی بر پایتون روی این سرور بیشتر می‌خوانید.

سرور VMware ESXi چیست؟

سرور VMware ESXi یک هایپروایزر هدفمند است که طیف گسترده‌ای از ویژگی‌های مهم سازمانی را ارائه می‌دهد. VMware ESXi مستقیما بر روی یک سرور فیزیکی قرار می‌گیرد و به آن اجازه می‌دهد تا به چندین ماشین مجازی تقسیم شود. این تکنولوژی به طور قابل توجهی نیاز به خرید یا ارتقا سخت‌افزار را کاهش می‌دهد. سرور VMware ESXi با دسترسی مستقیم و کنترل بر منابع زیرساخت، سخت افزار را تقسیم بندی می‌کند و به دنبال آن هزینه‌ها را کاهش می‌دهد.

تیم فناوری اطلاعات همواره برای برآورده کردن روندهای متغیر بازار و افزایش انتظارات مشتریان تحت فشار است. همچنین چالش‌هایی در رابطه با گسترش منابع IT برای انطباق با پروژه‌های جدید و پیچیده نیز وجود دارد. VMware ESXi به سازمان شما کمک می‌کند تا تعداد منابع سخت افزاری مورد نیاز برای اجرای هایپروایزر را کاهش دهد. علاوه بر این، به افزایش عملکرد کمک کرده و سخت افزار را برای استفاده از حداکثر ظرفیت بهینه می‌کند.

مزایای ESXi چیست؟

ESXi در حوزه مجازی سازی سرورها شناخته شده است و نتایج بسیار خوبی در این زمینه ارائه می‌دهد. ESXi با قابلیت‌های مقیاس پذیری منحصر به فرد به شما اجازه می‌دهد تا به طور ایمن روی یک یا چند ماشین مجازی کار کنید. همچنین برای سرورهای موقتی و در محیط های آزمایشی نیز مورد استفاده قرار می‌گیرد. با مجازی سازی می‌توانید در هزینه، منابع و فضا صرفه جویی کنید، بدون اینکه به امنیت سازمان شما لطمه‌ای وارد شود. عملکرد ESXi بسیار قوی است و به صورت بهینه از منابع موجود استفاده می‌کند. انعطاف پذیری بالا و نصب سریع از مزایای دیگر این فناوری است. لازم به ذکر است که با اجاره سرور ESXi می‌توانید حتی پول بیشتری پس انداز کنید.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

ویژگی‌های VMware ESXi

اندازه کوچک

Vmware سرور ESXi را به عنوان کوچک‌ترین هایپروایزر جهان معرفی می‌کند. این سرور کوچک اغلب به کاهش سطح حملات و تهدیدات خارجی کمک می‌کند و نگهداری آن بسیار آسان است.

نصب راحت

نصب ESXi به سرعت انجام می‌شود و می‌توانید زیرساخت خود را در سریع‌ترین زمان ممکن راه اندازی کنید.

ابزار مدیریتی کاربر پسند

ESXi یک مرورگر داخلی و سازگار با HTML5 برای استفاده سازمانی ارائه می‌دهد. همچنین سازمان‌هایی که به اتوماسیون نیاز دارند می‌توانند از رابط خط فرمان vSphere برای مدیریت از راه دور و API استفاده کنند.

پشتیبانی و سازگاری گسترده

محبوبیت ESXi به عنوان یک پلتفرم سازمانی به معنای پشتیبانی گسترده از سخت افزار و نرم افزار و همچنین سازگاری با طیف گسترده‌ای از برنامه‌ها و سیستم عامل‌هاست.

حمله به سرورهای VMware ESXi

به تازگی یک باج افزار مبتنی بر پایتون ناشناخته سرورهای VMware ESXi را هدف حمله قرار داده است. در این حمله هکرها دستورات رمزگذاری شده را از راه دور بر روی سیستم مورد نظر اجرا می‌کنند. این حمله سرور VMware ESXi و رمزگذاری ویرچوال دیسک‌ها را هدف قرار داد. این اسکریپت پایتون پس از اجرا بر روی hypervisor سازمان مورد نظر، همه ماشین‌های مجازی را از دسترس خارج می‌کند.

محققان دریافتند که ممکن است سرور با استفاده از رمزگذاری CVE-2019-5544 و CVE-2020-3992 در سرویس OpenSLP ESXiدر معرض خطر قرار گرفته باشد. باج افزار مبتنی بر پایتون از نظر فنی می‌تواند سیستم‌های لینوکس و یونیکس را نیز هدف قرار دهد، اما شواهد زیادی وجود دارد که نشان می‌دهد این حمله برای پلتفرم VMware ESXi طراحی شده است.

عملیات غیرقانونی مبتنی بر اسکریپت پایتون

باج افزار مبتنی بر پایتون هفت لاین را در داخل "/etc/rc.local.d/local.sh" اضافه می‌کند. این فایل ESXi در راه اندازی مجدد دوباره اجرا می‌شود و معمولا فایل خالی است. یکی از این خطوط تحت عنوان «/store/packages/vmtools.py» اسکریپت پایتون را راه‌اندازی می‌کند. تصاویر VM، گزارش‌ها و موارد دیگر در این اسکریپت ذخیره می‌شوند. محققان بر این باورند که بدافزارها با نام و مکان این اسکریپت سرورهای VMware ESXi را هدف قرار دادند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

حمله باج افزار مبتنی بر پایتون چگونه انجام شد؟

محققان می‌گویند اسکریپت پایتون در این حمله می‌تواند با اندکی تغییر در لینوکس یا سایر سیستم‌های مشابه یونیکس استفاده شود. نشانه‌های متعددی وجود دارد که این حمله به‌طور خاص برای هدف قرار دادن ESXi طراحی شده است. یک فایل با نام /store/packages/vmtools.py کاراکتر به کاراکتر از فایل پایتون ارائه شده توسط VMware نسخه برداری می‌کند.

این اسکریپت یک وب سرور راه اندازی می‌کند که درخواست‌های POST محافظت شده را از حملات راه دور دریافت می‌کند. این درخواست‌ها می‌توانند یک پوسته معکوس روی هاست راه‌اندازی کنند. پوسته معکوس به دور زدن محدودیت‌های فایروال کمک کرده یا در مورد اتصال شبکه را محدود می‌کند. یکی از اقدامات تهدید آمیز که توسط تحلیلگران Juniper مشاهده شد، تغییر پیکربندی پروکسی HTTP ESXi بود. این تغییر برای برقراری ارتباط با سرور از راه دور شکل گرفت.

برای تعیین اینکه آیا باج افزار مبتنی بر پایتون روی سرورهای ESXi تاثیر گذاشته است یا خیر، فایل‌های ذکر شده در بالا را در «local.sh» بررسی کنید. تمام فایل‌ها باید مورد بررسی قرار گرفته و به تنظیمات درست خود برگردند. در نهایت، ادمین باید تمام اتصالات ورودی شبکه را به هاست‌های قابل اعتماد محدود کرده و به روز رسانی‌های امنیتی را در اسرع وقت اعمال کند.

برترین مزایای VMware ESXi برای کسب و کارها

راه اندازی و مدیریت آسان و مقرون به صرفه

از آنجایی که VMware ESXi یک برنامه برای ایجاد ماشین‌های مجازی می‌باشد، راه اندازی آن آسان و سریع است. به کمک این سرور و استفاده از منابع فیزیکی اختصاصی فرایند مدیریت بسیار آسان می‌شود. به اشتراک گذاری منابع فیزیکی بین چندین ماشین مجازی، استفاده‌های سخت افزاری را آسان کرده و در عین حال هزینه‌ها را کاهش می‌دهد.

ایجاد محیط آزمایشی

با کمک VMware ESXi می‌توانید سرورهایی ایجاد کنید تا به‌روزرسانی‌های جدید را تست کند و در صورت نیاز آن‌ها را تغییر دهد تا امکان استفاده بیشتر از منابع فراهم شود. هر سرور به صورت جداگانه مورد استفاده قرار می‌گیرد و اجازه می‌دهد تا یک محیط آزمایشی خصوصی داشته باشید.

امنیت

امنیت VMware ESXi شاید مهم‌تر از کاربر پسند بودن آن باشد. عملکرد مدیریتی در VMkernel حمله دقیق با بدافزارها و سایر تهدیدات را شناسایی می‌کند؛ به این معنی که سیستم در برابر تهدیدات بسیار ایمن است و همچنین روز به روز قابل اعتمادتر می‌شود. برای انجام وظایف مدیریتی نیازی به یک حساب کاربری جامع نیست و در عوض می‌توان نقش‌ها و امتیازات را به حساب‌های فردی اختصاص داد. VMware ESXi همچنین به ماشین‌های مجازی ایجاد شده توسط Microsoft Virtual Server، Microsoft Virtual PC یا VMware Server اجازه می‌دهد روی ESXi کار کنند و همچنین از تبدیل ماشین‌های فیزیکی نیز پشتیبانی می‌کند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

نتیجه گیری

سرور ESXi "ستون فقرات" زیرساخت مجازی است و نظارت دقیقی بر عملکرد سیستم دارد تا از قطعی یا شناسایی حملات جلوگیری کند. ویژگی‌های ESXi می‌تواند مدیریت فناوری اطلاعات را ساده کند و نیازهای سخت‌افزاری را کاهش دهد. به همین خاطر است که ESXi به کارایی بیشتر با هزینه کمتر معروف است. حمله باج افزار مبتنی بر پایتون چالش جدیدی را ایجاد کرده. از اینکه این مقاله را مطالعه کردید متشکریم و امیدواریم که اطلاعات مفیدی در مورد vmware esxi به دست آورده باشید. شما از کدام هایپروایزر در محل کار خود استفاده می‌کنید و چرا؟

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net