**آینده امنیت سایبری در جهان**

آینده امنیت سایبری در جهان : با رشد مشاغل دیجیتال، خطر حملات سایبری به شدت افزایش می‌یابد. 25 درصد از شرکت‌ها در طول سال گذشته نقض امنیت سایبری را تجربه کرده‌اند. قابل توجه است که در این حوزه حتی 1 درصد هم می‌تواند ویرانگر باشد. شرکت‌هایی که مورد حملات سایبری قرار گرفته‌اند مجبور به پرداخت هزینه‌های سنگینی شده‌اند که بر اساس اطلاعات داده شده این رقم بیش از 60 میلیون دلار گزارش داده شده است.

افزایش [حملات سایبری](https://softyab.com/ransomware-attacks-on-hospitals-during-the-pendemic/) و افزایش آسیب پذیری‌های امنیتی، سازمان‌ها را مجبور کرده است تا از ایجاد هر گونه آسیب به داده‌های خود آن‌ها را متوقف کنند یا این که به هزینه‌های بالای حملات سایبری که می‌تواند منجر به آسیب جدی به فرایندهای کسب و کاری سازمان و آینده امنیت سایبری شود را قبول کنند.

بر اساس تحقیق‌های انجام شده، حملات سایبری آتی متشکل از ابزارهای مستقل از پیش برنامه نویسی شده‌ای هستند که با هدف آلوده کردن شبکه‌های سازمانی طراحی شده و تنها در عرض چند دقیقه می‌توانند اقدام به سرقت اطلاعات یا تخریب داده‌های سازمان‌ها کنند. در حال حاضر حتی سازمان‌هایی که از روش‌های توصیه شده نیز پیروی می‌کنند باز هم نیازمند حداقل چند ساعت زمان برای پاسخگویی به حوادث امنیتی هستند.

**حملات سایبری NotPetya**

به همین خاطر، مدافعان سایبری باید سرعت واکنش خود نسبت به آسیب‌های امنیتی را افزایش دهند. به عنوان مثال، حمله “NotPetya” که از بدافزاری به نام “[Petya](https://softyab.com/%D8%AA%D8%B9%D8%B1%DB%8C%D9%81-%D9%88%DB%8C%D8%B1%D9%88%D8%B3-%DB%8C%D8%A7%D8%A8-%D8%A7%D8%B2-%D8%B2%D8%A8%D8%A7%D9%86-g-data/)” استفاده می کرد، ابتدا فرایند به روز رسانی خودکار نرم افزار حسابداری شرکت MEDoc را مختل نموده و سپس به جای آن بدافزاری را نصب کرد که در کل شرکت منتشر شد.

اوایل، هدف حملات سایبری NotPetya، شرکت‌ها و سازمان‌های اوکراینی بود اما پس از این که شرکت MEDoc به بدافزار آلوده شد، این آلودگی به شرکت‌های بزرگ دیگری از جمله “Maersk” که یک شرکت دانمارکی است و در زمینه صنعت نفت فعالیت می‌کند نیز راه یافت. در شرکت Maersk تنها در مدت زمان بسیار کوتاهی، آلودگی توانست از یک نقطه کوچک به همه رایانه‌ها سرایت کند. در حالی که اجرای حمله، آلودگی سایر سیستم‌ها در شبکه، پیدا کردن منابع و استخراج آن‌ها فقط در دو ساعت و نیم انجام شد ولی عملیات پاکسازی رایانه‌های شرکت از این آلودگی علاوه بر این که هزینه‌های بسیار زیادی را به شرکت تحمیل کرد، حدوداً ۱۰ روز هم زمان برد. به همین دلیل است که در سازمان‌های بزرگ، انجام واکنش‌های سریع و خودکار به حملات سایبری امروزه امری بسیار ضروری به شمار می‌رود.

منظور از روش‌ها و راهکارهای توصیه شده که در بالا به آن اشاره شد، استفاده از ابزارهای مستقل برای مقابله با آسیب‌های امنیتی است که همه فعالیت‌ها از جمله تشخیص آلودگی در سریع‌ترین زمان ممکن، تصمیم گیری در خصوص نحوه واکنش به آن، شناسایی و تفکیک سیستم‌های آلوده، به روز رسانی قوانین فایروال، تقسیم بندی شبکه به منظور کنترل بهتر سازمان را در بر می‌گیرد. هر چند اعتماد کردن به این ابزارها ممکن است کار سختی باشد اما باید به سطحی از اعتماد و اطمینان رسید تا بتوان به صورت خودکار از فعالیت‌های کسب و کاری سازمان در مقابل نفوذهای سایبری محافظت کرد.

اولین اقدام در این خصوص نیز تلاش در جهت افزایش آگاهی و درک مدیران سازمان‌ها از مخاطرات امنیتی است. در نتیجه می‌توان آن‌ها را به خرید ابزارهای امنیتی خودکار و صرف هزینه در این زمینه متقاعد کرد. مدیر یکی از شرکت‌های بزرگ گفته است که با توجه به هزینه‌های مربوط به [فایروال‌ها](https://softyab.com/what-is-firewall/)، سیستم‌های IPS یا مقابله با نفوذ و همچنین ضدبدافزارها، درصد بسیار بالایی از بودجه امنیتی فعلی صرف پیشگیری از ایجاد صدمه به سازمان‌ها می‌شود.

بنابراین با توجه به احتمال بالای شکست در اتخاذ چنین رویکردی و به منظور کاهش آسیب‌های ناشی از حملات سایبری بهتر است سازمان‌ها توانایی‌های خود برای تشخیص و واکنش به موقع در هنگام وقوع حملات سایبری را بالا ببرند.

**بارگذاری بدافزارها و سرقت داده‌ها در فایل‌های تصویری**

**استگانوگرافی در آینده امنیت سایبری**

استگانوگرافی یکی از روش‌های پنهان کردن داده یا فایل، در فایلی دیگر در آینده امنیت سایبری میباشد که در آن فقط افرادی که از وجود فایل‌های مخفی باخبر هستند، قادر به استفاده از ابزارهای لازم جهت دستیابی به آن‌ها هستند. یک تیم امنیتی، حملاتی که در آن‌ها تعدادی از ابزارهای حمله، با استفاده از روش استگانوگرافی در فایلهای تصویری جایگذاری شده بودند را مورد بررسی قرار داده است.

نتایج تحقیقات این تیم بیانگر آن بوده که مهاجمان، بدافزارها و کدهای مخرب شان را با استفاده از الگوریتم‌های رمزنگاری بر روی فایل‌های تصویری پنهان می‌کنند. این فایل‌ها ظاهر معمولی داشته و روی یک دامنه مجاز و معتبر میزبانی می‌شوند. سپس آن‌ها توسط ابزارهای مدیریت و کنترل از راه دور (RAT) بدافزارهایشان را در شبکه‌های مورد نظر بارگذاری و نصب می‌کنند.

از آن جا که دانلود فایل‌های تصویری از یک سرور و دامنه مجاز، منجر به فعال شدن سامانه‌های نظارت امنیتی نمی‌شود پس مورد مشکوک و خاصی هم مشاهده نخواهد شد. بنابراین با توجه به این که کل این فرایند به صورت مخفیانه انجام می‌شود، دور زدن کنترل‌های امنیتی آسان بوده و تشخیص آن نیز برای سازمان‌ها کار نسبتاً سختی است.

با استفاده از این روش می‌توان هر نوع فایلی از جمله بدافزارهایی که مهاجم در مراحل بعدی حمله نیازمند آن‌ها است، قطعه کدهایی که می‌بایست بر روی سیستم قربانی اجرا شوند یا فرمان‌هایی که برای پیکربندی مجدد زیرساخت‌ها مورد استفاده قرار می‌گیرند را مخفی کرد.

بر اساس سایر نتایج تحقیقات این تیم امنیتی، در حمله‌های سایبری خودکار از روش استگانوگرافی برای استخراج داده‌ها از شبکه نیز استفاده شده است. در واقع داده‌های به سرقت رفته، در فایل‌های تصویری کدگذاری شده و سپس در یک پوشه در وب سایت سازمان قرار گرفته‌اند که مهاجمان به راحتی توانسته‌اند آن‌ها را دانلود کنند.هوش مصنوعی در حال بازتعریف جنبه‌های مختلف امنیت سایبری است. همچنین قابل ذکر است یادگیری ماشین که به‌عنوان یکی از زیرشاخه‌های اصلی هوش مصنوعی شناخته می‌شود از ارتقاء توانایی سازمان‌ها در پیش‌بینی و خنثی کردن تخلفات، تا جلوگیری از تکثیر سطوح تهدید با چارچوب‌های امنیتی مبتنی بر اعتماد صفر و ساختن واژگان عبور موقتی و... برای تأمین امنیت محیط‌های تجاری، زیرساختی و حتی خانگی پشتیبانی می‌کند.

منبع: [infosecurity-magazine](https://www.infosecurity-magazine.com/news/passwordless-authentication/)

لطفا جهت مشاوره در [انتخاب آنتی ویروس مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[اجتماعی](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**