گروه هکر ایرانی چطور شرکت آمریکایی سیتریکس را هک کرد؟ - دیجیاتو

آرش پارساپور | شنبه، ۱۷ فروردین ۱۳۹۸

گروهی موسوم به ایریدیوم در دو حمله آذر و اسفند ماه خود شرکت سیتریکس را مورد حمله قرار داده و بیش از ۶ ترابایت از اطلاعات محرمانه این شرکت را به سرقت بردند. کارشناسان امنیت اطلاعات معتقدند که این موضوع می‌تواند سیاسی باشد چرا که این گروه‌های به اصطلاح APT معمولا توسط دولت‌ها حمایت می‌شوند. آنها همچنین امروز که چند وقتی از این حمله می‌گذرد جزییات بیشتری از نحوه این حمله را توضیح داده‌اند.

گفتنیست شرکت سیتریکس یک شرکت نرم‌افزار آمریکایی است، که در زمینه ارائه خدمات سرورها و شبکه‌های رایانه‌ای، سامانه‌های کنترل از راه دور رایانه و رایانش ابری، ارائه نرم‌افزارهای شناسایی یگانه، سرورهای کاربردی، ترمینال رایانه، نرم‌افزارهای مالکیتی، نرم‌افزارهای مجازی‌سازی و مجازی‌سازی شبکه فعالیت می‌کند.

«جواد دادگر» یکی از کارشناسان فنی و آگاه نسبت به این حمله است و در گفتگو با دیجیاتو روش Password Spraying را روش هکرهای ایریدیوم معرفی می‌کند و می‌گوید که دادن لقب ایریدیوم به این گروه از سوی کاشفین حمله رخ داده، نه اینکه خود گروه چنین اسمی روی خود بگذارند و این گروه‌ها حتی الامکان با هویت و اسامی مجهول کار خود را می‌کنند:

> *«در این روش معمولا پسوردهای شناخته شده و مهم را برای تعداد بسیاری اکانت استفاده میکنند. این پسورد ها هرچی به نسبت هدف مشخص شده شخصی سازی شده تر باشه نتیجه بهتری در بر خواهد داشت. به طور مثال پسورهای زیاد استفاده شده‌ای چون ۱۲۳۴ و admin رو برای چند هزار تا اکانت تست میکنند و در یک مورد به جواب می‌رسند.»*

او باور دارد که در طی حملاتی از گذشته یک سری اطلاعات از کارمندان شرکت سیتریکس مورد سرقت قرار گرفته و پسوردها شخصی سازی شده و پرکاربردی مانند اسامی حیوانات خانگی یا تاریخ تولدها و... استخراج شده و از آنها در روش Password Spraying استفاده شده است.

احتمال دیگری که دادگر می‌دهد اینست که هکرهای گروه ایریدیوم توانسته‌اند VPN های مربوط به شرکت را پیدا کرده باشند و از طریق آنها به شبکه داخلی شرکت و Storageها وصل شوند:

«معمولا اطلاعات حتی داخل شرکت های اینچنینی نیز دارای طبقه بندی خاصی است. ممکن است VPN یک کارمند به اطلاعات خاصی دسترسی نداشته باشد و برای یک کارمند دیگر به اطلاعات محرمانه برسد. در هر صورت به طور قطع اطلاعات حیاتی مهمی به سرقت رفته است. آنطور که به نظر می‌آید هکرهای ایریدیوم به بیش از ۲۰۰ آژانس دولتی، شرکت‌های نفت و گاز و شرکت‌های فناوری از جمله شرکت سیتریکس سیستم آسیب زده‌اند.»

دادگر تاکید دارد که گروه ایریدیوم یکی از سرورهای میزبان اطلاعات سیتریکس را مورد هدف قرار داده‌اند که شامل مکاتبات ایمیلی، فایل‌های به اشتراک گذاشته شده در شبکه و دیگر سرویس‌های مورد استفاده برای مدیریت پروژه و تدارکات است.

دادگر احتمال سیاسی بودن این حملات را دور از ذهن نمی‌داند و با اشاره به گزارشات متعدد گروه‌های امنیت بین‌المللی می‌گوید که گروه ریسکوریتی نیز در بیانیه تحقیقی خود چنین آورده است: «این حملات، بخشی از یک کمپین جاسوسی پیچیده است و با توجه به اینکه یک دولت، مجموعه‌های نظامی و صنعتی، شرکت‌های انرژی، موسسات مالی و شرکت‌های بزرگ اقتصادی را هدف قرار داده، مشخصا می‌توان گفت که توسط یک دولت پشتیبانی می‌شود.»

گرچه سیتریکس تاکید کرده که نشانه‌ای دال بر سرقت اطلاعات مهم وجود ندارد اما کارشناسان بر این باورند که به احتمال زیاد اطلاعات گسترده‌ای از این سازمان لو رفته است. همچنین نگرانی اصلی این احتمال است که سیتریکس به عنوان پیمانکار بزرگ دولتی در زمینه طراحی شبکه و سرویس های ابری، داده های حساسی را در شرکت های دیگر نیز ذخیره کرده باشد.

دیجیاتو