

[View the original article](#)

از گوشه و کنار جهان

از رایانه‌های روسی تا لپ‌تاپ هانتر بایدن؛ چه کسانی پشت نرم‌افزار مرموز روسی هستند؟

راديو اروپاي آزاد/راديو آزادي

۱۴۰۵/مهر/۱۵



وبسایت آمریکایی شرکت اکسیژن فورنسیکس پس از اعلام اتهامات علیه دو مدیر اجرایی که ظاهراً در مورد مالکیت روسی این شرکت به دولت آمریکا دروغ گفته بودند، مسدود شد

یک نرم‌افزار قدرتمند استخراج اطلاعات دیجیتال که سال‌ها در اختیار نهادهای امنیتی و پلیسی آمریکا و اروپا بوده، اکنون در مرکز یک پرونده جنایی در ایالات متحده قرار گرفته است. مقام‌های آمریکایی می‌گویند شرکتی که این نرم‌افزار را عرضه می‌کرد، مالکیت و کنترل روسی خود را پنهان کرده بود.

گزارش اختصاصی راديو اروپاي آزاد/راديو آزادي نشان می‌دهد نرم‌افزار شرکت «اکسیژن فورنسیکس» (Oxygen Forensics) که قادر است اطلاعات تلفن‌های همراه، رایانه‌ها و دیگر وسایل الکترونیکی را استخراج کند و حتی از سد رمزهای عبور بگذرد، در سال‌های گذشته به‌طور گسترده در اختیار نهادهای دولتی و امنیتی آمریکا و اروپا بوده است.

وزارت دفاع آمریکا، سرویس مخفی، وزارت امنیت داخلی، اف‌بی‌آی و ده‌ها نهاد پلیسی فدرال و محلی در آمریکا و اروپا از جمله مشتریان این نرم‌افزار بوده‌اند.

اما وزارت دادگستری آمریکا در ماه سپتامبر دو مدیر شرکت اکسیژن فورنریکس را متهم کرد که درباره مالکیت و کنترل واقعی شرکت به دولت آمریکا اطلاعات نادرست داده‌اند.

بر اساس اتهام‌های مطرح‌شده، این شرکت در واقع در مالکیت و کنترل اتباع روسیه بوده است.

این پرونده اکنون پرسش‌هایی جدی درباره امنیت نرم‌افزاری مطرح کرده که برای دسترسی به برخی از حساس‌ترین داده‌های دیجیتال مورد استفاده قرار گرفته است؛ هرچند تا این لحظه هیچ مدرک علنی‌ای منتشر نشده که نشان دهد این نرم‌افزار حاوی کد مخرب یا «در پشتی» برای دسترسی پنهانی به اطلاعات بوده است.

ابزاری برای شکستن قفل تلفن و رایانه

یکی از نمونه‌هایی که توانایی این نرم‌افزار را نشان می‌دهد، به لپ‌تاپ هانتر بایدن، پسر جو بایدن، رئیس‌جمهور پیشین آمریکا، مربوط است.

در اکتبر ۲۰۲۴، کنستانتینوس «گاس» دیمیتریلوس، مأمور پیشین سرویس مخفی آمریکا، در یک نشست تخصصی در ویرجینیا نرم‌افزار اکسیژن فورنریکس را برای گروهی از متخصصان فناوری معرفی کرد.

در ویدئویی از این نشست که به دست رادیو اروپای آزاد/رادیو آزادی رسیده است، دیمیتریلوس گفت از اکسیژن فورنریکس برای بررسی نسخه‌ای از هارددیسک لپ‌تاپ هانتر بایدن استفاده کرده و توانسته است ده‌ها هزار فایل از جمله شمار زیادی فایل حذف‌شده را از آن بازیابی کند.

او می‌گوید: «اکسیژن ابزار شماره یک من است. تنها ابزاری است که استفاده می‌کنم و تنها ابزاری است که تدریس می‌کنم. عاشقش هستم.»

دیمیتریلوس توضیح می‌دهد یکی از دلایل استفاده از این نرم‌افزار این است که به او امکان می‌دهد داده‌ها را بازیابی و اصالت آن‌ها را بررسی کند.

روزنامه واشینگتن اگزمینر دیمیتریلوس را برای بررسی هارددیسک هانتر بایدن به کار گرفته بود. او مدعی شد با استفاده از اکسیژن فورنریکس فایل‌های بیشتری، از جمله ده‌ها هزار فایل حذف‌شده، نسبت به بررسی‌های قبلی بازیابی کرده است.

پیش از آن، اف‌بی‌آی مالکیت لپ‌تاپ را تأیید کرده و واشینگتن پست نیز با استفاده از کارشناسان مستقل بخشی از داده‌های آن را بررسی کرده بود.

نسخه آمریکایی، همان نسخه روسی

موضوع زمانی حساس‌تر شد که مشخص شد نسخه‌ای که در آمریکا عرضه می‌شد، بنا بر گفته فعالان روسی و یک کارمند سابق شرکت، همان نرم‌افزاری است که در روسیه نیز ارائه می‌شود.

این نرم‌افزار در روسیه در اختیار سرویس امنیت فدرال، اف‌اس‌بی، و دیگر نهادهای حکومتی قرار گرفته است.

پنج شهروند روسیه که نام آن‌ها به‌عنوان مالکان شرکت روسی «ام‌کی‌او سیستمز» ثبت شده، همان افرادی هستند که مقام‌های آمریکایی می‌گویند پشت شرکت اکسیژن فورنریکس نیز قرار داشته‌اند.

یکی از این افراد، اولگ داویدوف، مدیر ارشد فناوری شرکت و شهروند روسیه است که در فرودگاه هیترو لندن بازداشت شده و در انتظار روند احتمالی استرداد به آمریکا در زندان است.

لی رایبر، مدیرعامل آمریکایی اکسیژن فورنیزیکس، نیز همان روز در ایالت آیداهو بازداشت و سپس با قرار وثیقه آزاد شد.

سرویس مخفی آمریکا در ماه فوریه قرارداد پنج‌ساله خود با این شرکت را با اشاره به «خطرات امنیتی» لغو کرده بود.

در مقابل، وزارت خارجه آمریکا در ماه اوت، تنها چند هفته پیش از اعلام اتهام‌های کیفری، قرارداد تازه‌ای با این شرکت امضا کرده بود.

پس از علنی شدن پیشینه روسی شرکت، شماری از نهادهای پلیسی در بریتانیا و دیگر کشورهای اروپایی نیز برای توقف استفاده از نرم‌افزار اقدام کردند.

بیشتر در این باره:

مقامات آمریکایی: شرکت فروشنده نرم‌افزار به پنتاگون مالکیت روسی خود را پنهان کرده بود



آیا «در پشتی» وجود داشته است؟

یکی از مهم‌ترین پرسش‌های امنیتی درباره این نرم‌افزار این است که آیا امکان دسترسی پنهان سازندگان روسی به داده‌های استخراج‌شده وجود داشته یا نه.

رونا سندویک، کارشناس نروژی-آمریکایی امنیت دیجیتال، می‌گوید صرف روسی بودن مالکان یک شرکت به این معنا نیست که نرم‌افزار آن الزاماً فعالیت مشکوکی انجام داده است.

او تأکید کرده است: «هیچ مدرک محکمی نداریم که نشان دهد نرم‌افزار کاری غیر از آنچه قرار بوده انجام دهد، انجام داده است.»

با این حال، سندویک ساختار مالکیت شرکت را غیرعادی توصیف کرده و گفته شرکت‌های معتبر معمولاً به چنین شیوه‌ای سازمان‌دهی نمی‌شوند.

وزارت دادگستری آمریکا نیز در اعلام اتهام‌های خود تصریح کرده که شکایت کیفری مدعی نیست نرم‌افزار اکسیژن دارای کد مخرب بوده یا برای دسترسی غیرمجاز به اطلاعات استفاده شده است.

سرویس مخفی آمریکا نیز در پاسخ به رادیو اروپای آزاد/رادیو آزادی گفته است استفاده از این نرم‌افزار در فوریه ۲۰۲۶، پس از شناسایی خطرات امنیتی، بلافاصله متوقف شد.

این نهاد افزوده نرم‌افزار فقط در محیط‌های موسوم به «ایرگپ» استفاده شده؛ یعنی شبکه‌هایی که از اینترنت و دیگر شبکه‌های ناامن جدا هستند.

به‌گفته سرویس مخفی آمریکا، هیچ مدرکی وجود ندارد که اطلاعات حساس در معرض خطر قرار گرفته باشد.

اما ماریان میگر، که مسئول فروش محصولات اکسیژن فورنزیکس به نهادهای دولت فدرال آمریکا بود، می‌گوید از مالکیت و کنترل روسی شرکت اطلاعی نداشته است.

او با اشاره به قدرت بالای نرم‌افزار گفته است اگر ابزاری بتواند به «تقریباً هر چیزی» نفوذ کند، این‌که سازندگان و مالکان آن روس باشند مسئله‌ای جدی ایجاد می‌کند.

سندویک نیز گفته ایجاد یک «در پشتی» از نظر فنی امکان‌پذیر است، هرچند به باور او نهادهای آمریکایی باید توانایی شناسایی و جلوگیری از چنین اقدامی را داشته باشند.

ریشه‌های روسی شرکت

ریشه شرکت به سال ۲۰۰۲ در روسیه بازمی‌گردد؛ زمانی که اولگ داویدوف و اولگ فیودوروف شرکتی به نام Oxygen Software تأسیس کردند.

یکی از بنیان‌گذاران ثبت‌شده این شرکت «مؤسسه پژوهشی ارتباطات رادیویی مسکو» بود؛ نهادی دولتی در دوره شوروی که در زمینه سامانه‌های ارتباط ماهواره‌ای و تجهیزات الکترونیکی موشکی فعالیت داشت و در دهه ۱۹۹۰ خصوصی شد.

شرکت اکسیژن تا سال ۲۰۱۵ در ساختمان همین مؤسسه مستقر بود و سپس نام واحد روسی خود را به «ام‌کی‌او سیستمز» تغییر داد.

داویدوف دو سال پیش از آن، شرکت Oxygen Forensics را در حومه واشینگتن در ایالت ویرجینیا راه‌اندازی کرده بود.

در روسیه، نرم‌افزار این شرکت به یکی از ابزارهای مهم جرم‌یابی دیجیتال تبدیل شد و نهادهایی چون کمیته تحقیقات، وزارت کشور و اف‌اس‌بی از آن استفاده کردند.

استفاده در پرونده‌های سیاسی در روسیه

فعالان و کارشناسان می‌گویند نسخهٔ روسی این نرم‌افزار به‌طور گسترده برای شکستن قفل وسایل الکترونیکی مورد استفاده قرار گرفته و در مواردی نیز در پرونده‌های دارای انگیزه سیاسی به کار رفته است.

یکی از افرادی که دستگاه‌های الکترونیکی او هدف چنین بررسی‌هایی قرار گرفت، آلسو کورماشوا، روزنامه‌نگار رادیو اروپای آزاد/رادیو آزادی، بود.

او در سال ۲۰۲۳ هنگام سفر به روسیه بازداشت و بعداً به شش سال و نیم زندان محکوم شد؛ اتهام‌هایی که خود او و رادیو اروپای آزاد/رادیو آزادی بی‌اساس می‌دانستند.

کورماشوا در اوت ۲۰۲۴ در جریان تبادل زندانیان آزاد شد.

تلاش برای پنهان کردن مالکیت پس از جنگ اوکراین

در آمریکا، اکسیژن فورنزیکس قراردادهای پرسودی با نهادهای مختلف دولتی، از جمله وزارت امنیت داخلی و سرویس مخفی، به دست آورد.

بر اساس اسناد داخلی فروش که در اختیار رادیو اروپای آزاد/رادیو آزادی قرار گرفته، این شرکت با ده‌ها نهاد فدرال و ایالتی آمریکا و شمار زیادی از سازمان‌ها در دیگر کشورهای جهان قرارداد داشته است.

دادستان‌های آمریکایی می‌گویند پس از آغاز تهاجم تمام‌عیار روسیه به اوکراین در سال ۲۰۲۲، شرکت برای جلوگیری از دست دادن قراردادهای دولتی آمریکا کوشید مالکیت روسی خود را پنهان کند.

به گفته دادستان‌ها، یک شرکت واسطه با نامی مشابه در قبرس تأسیس شد و نام پنج مالک روس نیز از اسناد شرکتی در روسیه حذف شد.

با این حال، مقام‌های آمریکایی می‌گویند این افراد همچنان در تصمیم‌گیری‌های شرکت، کنترل پرداخت‌ها و نظارت بر حساب‌های بانکی نقش داشتند.

لی رابیر، مدیرعامل آمریکایی شرکت، نیز متهم شده است که در سال‌های ۲۰۲۲ و ۲۰۲۳ به دولت آمریکا گواهی داده بود اکسیژن فورنزیکس مالک دیگری ندارد؛ موضوعی که برای دریافت قراردادهای دولت فدرال اهمیت اساسی داشت.

پرونده‌ای که تازه باز شده است

اکنون پس از سال‌ها استفاده گسترده از نرم‌افزار اکسیژن فورنزیکس در آمریکا و اروپا، پرونده مالکیت شرکت توجه نهادهای امنیتی و پلیسی را به خود جلب کرده است.

هنوز هیچ مدرکی منتشر نشده که نشان دهد اطلاعات استخراج‌شده با این نرم‌افزار در اختیار نهادهای روسی قرار گرفته یا از نرم‌افزار برای جاسوسی استفاده شده است.

اما اتهام پنهان کردن مالکیت و کنترل روسی شرکتی که نرم‌افزار آن برای شکستن قفل تلفن‌ها و رایانه‌ها و دسترسی به اطلاعات حساس به کار می‌رود، اکنون به‌خودی خود به یک نگرانی امنیتی جدی برای دولت‌های غربی تبدیل شده است.

نمونهٔ لپ‌تاپ هانتر بایدن تنها یکی از مواردی است که نشان می‌دهد این نرم‌افزار چه توانایی‌هایی دارد؛ ابزاری که به‌گفتهٔ کارشناس استفاده‌کننده از آن توانسته ده‌ها هزار فایل از جمله اطلاعات حذف‌شده را بازیابی کند و در همان حال نسخه‌ای از همین فناوری در اختیار نهادهای امنیتی روسیه نیز بوده است.

این مطلب بخشی از:

فراتر از خبر

از گوشه و کنار جهان

بایگانی